T.C
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
YÖNETİM VE ORGANİZASYON PROGRAMI
YÜKSEK LİSANS TEZİ

HACKTİVİZM OLGUSU VE KURUMSAL İTİBAR İLİŞKİSİ ÜZERİNE KURAMSAL BİR İNCELEME

ÜMİT YEŞİL

Danışman
Yrd. Doç. Dr. Nurcan HAKAN ÇIRAKLAR

İZMİR - 2016

YÜKSEK LİSANS
TEZ/ PROJE ONAY SAYFASI

2012801886

Üniversite : Dokuz Eylül Üniversitesi

Enstitü : Sosyal Bilimler Enstitüsü

Adı ve Soyadı : Ümit YEŞİL

Tez Başlığı : Hacktivizm Olgusu ve Kurumsal İtibar İlişkisi Üzerine Kuramsal Bir İnceleme

Savunma Tarihi : 26.02.2016

Danışmanı : Yrd.Doç.Dr.Nurcan Hakan ÇIRAKLAR

JÜRİ ÜYELERİ

Ünvanı, Adı, Soyadı	Üniversitesi	İmza
Yrd.Doç.Dr.Nurcan Hakan ÇIRAKLAR	DOKUZ EYLÜL ÜNİVERSİTESİ	
Doç.Dr.Ethem DUYGULU	DOKUZ EYLÜL ÜNİVERSİTESİ	
Yrd.Doç.Dr.Evrim MAYATÜRK AKYOL	İZMİR KATİP ÇELEBİ ÜNİVERSİTESİ	

Oybirliği (X)

Oy Çokluğu ( )

Ümit YEŞİL tarafından hazırlanmış ve sunulmuş "**Hacktivizm Olgusu ve Kurumsal İtibar İlişkisi Üzerine Kuramsal Bir İnceleme**" başlıklı Tezi(X) / Projesi( ) kabul edilmiştir.

Prof.Dr. Mustafa Yaşar TINAR
Enstitü Müdürü

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum "Hacktivizm Olgusu ve Kurumsal İtibar İlişkisi Üzerine Kuramsal Bir İnceleme" adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

Tarih
15/02/2016
Ümit YEŞİL

ÖZET

Hacktivizm Olgusu ve Kurumsal İtibar İlişkisi Üzerine Kuramsal Bir İnceleme

Ümit YEŞİL

Dokuz Eylül Üniversitesi
Sosyal Bilimler Enstitüsü
İşletme Anabilim Dalı
Yönetim ve Organizasyon Programı

Hack eylemi ve aktivizmin birleşimini temsil eden hacktivizm olgusu, "şiddet içermeyen ancak suç teşkil eden hack tekniklerinin politik bir gündem amacıyla kullanılması" olarak tanımlanmaktadır. Bu eylemleri gerçekleştiren bireyler (veya gruplar) hacktivist olarak adlandırılmakta ve gerçekleştirdikleri hack eylemleri vasıtasıyla; hükümetlere, küresel kuruluşlara, işletmelere ve genel olarak topluma mesajlarını duyurmaya çabalamaktadırlar. Bu eylemler kimi zaman eylemin hedefindeki kurumlara finansal kayıpların yanında itibari kayıplar da yaşatmaktadır. Bu sebeple, hacktivist eylemler ve kurumsal itibar arasındaki ilişkileri ortaya çıkarmak önem kazanmaktadır.

Alan yazında, hacktivist eylemlerin kurumsal itibara zarar vereceğine sıklıkla değinilmesine rağmen, hacktivizm ve kurumsal itibar arasındaki bağlantıların anlaşılması üzerine bütünleştirici bir model kapsamında ele alınan pek fazla araştırmaya rastlanılmamıştır. Dolayısıyla, bu çalışmanın amacı, hacktivizm olgusu ve kurumsal itibar ilişkisini incelemektir. Çalışmanın kapsamını, kar amacı gütmeyen kurumlardan ziyade kar amacı güden kuruluşlar oluşturmaktadır.

Bu çalışmada, hacktivizm ve kurumsal itibar ilişkisini daha iyi anlayabilmek adına, öncelikle hacktivizm ve kurumsal itibar kavramları tüm yönleriyle ele alınmakta, sonrasında ise, her iki kavram arasındaki ilişki detaylı olarak incelenmektedir. Son bölümde ise, PytlikZillig ve diğerlerinin (2014) "Hacktivizme Destek/Direnç Modeli" ile Schwaiger'in (2004) "Kurumsal İtibar Modeli"ne bağlı olarak, bütüncül bir bakış açısıyla hacktivizm ve kurumsal itibar ilişkisine yönelik bir model önerisi geliştirilmektedir.

Çalışma, metodolojik açıdan ilgili yerli ve yabancı yazın taramasına dayalı olmak üzere, hacktivizm ve kurumsal itibar ilişkisini kuramsal bir bakış açısıyla ele almakta ve geliştirilen model önerisiyle yazına önemli bir katkı sağlayacağı ve bu yönüyle özgün ve gelecekteki araştırmacılar ve uygulamacılar için yol gösterici bir niteliğe sahip olduğu düşünülmektedir.

Anahtar Kelimeler: Hacktivizm, Çevrimiçi Aktivizm, Elektronik Sivil İtaatsizlik, Kurumsal İtibar, Kurumsal İmaj, Kurumsal Kimlik.

ABSTRACT

A Theoretical Study on The Relationship Between The Hacktivism Phenomenon and Corporate Reputation

Ümit YEŞİL

Dokuz Eylül University
Graduate School of Social Sciences
Department of Business Administration
Management and Organization Program

The hacktivism phenomenon, which implies the marriage of hacking and activism, is defined as "the nonviolent use of illegal or legally ambigous digital tools in pursuit of political ends". The individuals (or groups) who are the actors of such hack actions are being called as hacktivists and those actions that they carry out is simply a struggle to spread their political message to the institutions like governments, global organizations and corporations along with the whole society. Those actions in the end, cause some financial and reputational damage occasionally. Hence, it gets more important to study the links between those hacktivist actions and corporate reputation.

Even though it is constantly stated in the literature that hacktivist actions may cause reputational damage, there is a lack of holistic studies on the possible relations between the phenomenon of hacktivism and the concept of corporate reputation. Thus, the purpose of this study is to fill this gap by uncovering the potential links between hacktivism and corporate reputation. The context of this study is limited with the profit-oriented organizations, in otherwords non-profit organizations are not included in this context.

In this study, first step is to provide a better understanding with a careful examination of the phenomenon of hacktivism and the concept of corporate reputation and once that is achieved, the possible links between those concepts are being examined. By the help of a holistic approach on two models, one of which is the "Hacktivism Support/Resistance Model" developed by PytlikZillig

et. al. (2014) and the other is "Corporate Reputation Model" developed by Schwaiger (2004), it is being aimed to develop a theoretical model explaining the relationships between hacktivism and corporate reputation.

This study, based on literature review, brings a theoretical approach to the relationships between hacktivism and corporate reputation. It is also considered to contribute to the existing literature especially with the theoretical model it proposed, hence it is seen as a unique study and thought to be a pioner one for future researchs.

Keywords: Hacktivism, Online Activism, Electronic Civil Disobedience, Corporate Reputation, Corporate Image, Corporate Identity.

HACKTİVİZM OLGUSU VE KURUMSAL İTİBAR İLİŞKİSİ ÜZERİNE KURAMSAL BİR İNCELEME

İÇİNDEKİLER

TEZ ONAY SAYFASI ii
YEMİN METNİ iii
ÖZET iv
ABSTRACT vi
İÇİNDEKİLER viii
KISALTMALAR xi
TABLOLAR LİSTESİ xii
ŞEKİLLER LİSTESİ xiii

GİRİŞ 1

BİRİNCİ BÖLÜM
HACKTİVİZM KAVRAMININ TANIMI, ANLAMI VE DİĞER KAVRAMLARLA İLİŞKİSİ, TARİHSEL GELİŞİMİ VE HACKTİVİZME TİPOLOJİK YAKLAŞIMLAR

1.1. HACKTİVİZM KAVRAMININ TANIMI VE ANLAMI 4
1.2. HACKTİVİZM KAVRAMININ DİĞER KAVRAMLARLA İLİŞKİSİ 7
1.2.1. Hacktivizm ve Elektronik Sivil İtaatsizlik 7
1.2.2. Hacktivizm ve Sanal Terörizm 9
1.2.3. Hacktivizm ve Çevrimiçi Aktivizm 10
1.2.4. Hacktivizm, Sanal Saldırı ve Sanal Savaş 12
1.2.5. Hacktivizm ve Sanal Casusluk 13
1.3. HACKTİVİZMİN TARİHSEL GELİŞİMİ 14
1.4. HACKTİVİZME YÖNELİK TİPOLOJİK YAKLAŞIMLAR 19
1.4.1. Samuel'in (2004) Hacktivizme Tipolojik Yaklaşımı 20
1.4.1.1. Hacktivistlerin Kökenleri 20
1.4.1.1.1. Hacker-Programcı Köken 21

1.4.1.1.2. Sanatçı-Aktivist Köken 22
1.4.1.2. Hacktivistlerin Yönelimleri 23
1.4.1.3. Samuel'in (2004) Tipolojisi 24
1.4.1.3.1. Politik Kırıcılar 25
1.4.1.3.2. Edimsel Hacktivizm 26
1.4.1.3.3. Politik Kodlayıcılar 27
1.4.2. Jordan ve Taylor'ın (2004) Hacktivizme Tipolojik Yaklaşımı 29
1.4.2.1. Kitlesel Eylem Hacktivizmi 30
1.4.2.2. Dijital Doğruculuk Hacktivizmi 32

İKİNCİ BÖLÜM
KURUMSAL İTİBAR KAVRAMI, TANIMI VE ANLAMI, DİĞER KAVRAMLARLA İLİŞKİSİ, KURUMSAL İTİBAR KAVRAMINA YAKLAŞIMLAR VE KURUMSAL İTİBARIN ÖLÇÜMÜ

2.1. KURUMSAL İTİBAR KAVRAMI, TANIMI VE ANLAMI 35
2.2. KURUMSAL İTİBAR, KURUMSAL KİMLİK VE KURUMSAL İMAJ KAVRAMLARI ARASINDAKİ İLİŞKİ 38
2.3. KURUMSAL İTİBAR YAKLAŞIMLARI 42
2.3.1. Gotsi ve Wilson'ın (2001) Kurumsal İtibar Yaklaşımı 44
2.3.2. Chun'un (2005) Kurumsal İtibar Yaklaşımı 46
2.3.3. Rindova, Williamson, Petkova ve Sever (2005) Yaklaşımı 49
2.3.4. Diğer Sınıflandırmalar 51
2.4. KURUMSAL İTİBARIN ÖLÇÜMÜ 53
2.4.1. Sıralama Bazlı Ölçümler 54
2.4.1.1. Fortune İtibar Endeksi (AMAC ve WMAC) 55
2.4.1.2. Management Today Britanya'nın En Çok Hayranlık Duyulan Şirketleri (BMAC) Endeksi 55
2.4.1.3. Harris-Fombrun İtibar Katsayısı (Reputation Quotient) ve Reputation Institute 56
2.4.2. Diğer Ölçümler 57
2.4.3. Kurumsal İtibar Ölçümlerine Yönelik Eleştiriler 59

ÜÇÜNCÜ BÖLÜM

HACKTİVİZM VE KURUMSAL İTİBAR İLİŞKİSİNE YÖNELİK YAZINA BİR BAKIŞ VE KURAMSAL BİR MODEL ÖNERİSİ

3.1. HACKTİVİZM VE KURUMSAL İTİBAR İLİŞKİSİNE YÖNELİK YAZINA BİR BAKIŞ 61

3.2. HACKTİVİZM VE KURUMSAL İTİBAR İLİŞKİSİ YAZININA DAYALI KURAMSAL BİR MODEL ÖNERİSİ 63

SONUÇ 76

KAYNAKÇA 81

KISALTMALAR

ABD	Amerika Birleşik Devletleri
AMAC	America's Most Admired Companies
BMAC	Britain's Most Admired Companies
CAE	Critical Art Ensemble
cDc	Cult of the Dead Cow
DDoS	Distributed Denial of Service
DoS	Denial of Service
DTÖ	Dünya Ticaret Örgütü
EDT	Electronic Disturbance Theatre
IMF	Uluslararası Para Fonu
LoU	Legion of the Underground
MIT	Massachusetts Institute of Technology
NASA	National Aeronautics and Space Administration
WMAC	World's Most Admired Companies
YIPL	Youth International Party Line

TABLOLAR LİSTESİ

Tablo 1: Hackerlara Verilen Farklı Etiketler s. 5
Tablo 2: Hacktivizmin Evrimindeki Önemli Olaylar s. 18
Tablo 3: Hacktivist Yönelimlerin Özellikleri s. 23
Tablo 4: Hacktivistlerin Kökenleri ve Yönelimlerine Göre Hacktivizm Tipleri s. 24
Tablo 5: Gotsi ve Wilson'ın (2001) Kurumsal İtibar Yaklaşımı s. 46
Tablo 6: Chun'un (2005) Kurumsal İtibar Yaklaşımı s. 48
Tablo 7: Rindova ve Diğerlerinin (2005) Kurumsal İtibar Yaklaşımı s. 50
Tablo 8: Bir Bütün Olarak Kurumsal İtibara Farklı Yaklaşımlar s. 52

ŞEKİLLER LİSTESİ

Şekil 1: Hacktivizmin Sınırları s. 11
Şekil 2: Kurumsal İtibarın Unsurları s. 42
Şekil 3: Hacktivizme Destek ve Direnç Modeli s. 64
Şekil 4: Hacktivizm ve Kurumsal İtibar İlişkisi Üzerine Geliştirilen Model s. 75

GİRİŞ

Son yıllarda pek çok firma hack saldırılarına maruz kalmakta ve bu saldırılar firmalara finansal kayıpların yanında itibari kayıplar da yaşatmaktadır. Bu saldırıların çoğu firmaların faaliyetlerine tepki olarak değil, bireysel kazanç sağlamak adına yapılmaktadır. Ancak bazı saldırılar doğrudan firmaların faaliyetlerinden doğan hoşnutsuzluğu göstermek adına gerçekleştirilmekte (Papadimitriou, 2009: 1332) ve özellikle bu firmaların itibarlarını zedelemek için yapılmaktadır (Advisen, 2012: 2). Hack eylemlerini bireysel kazanç için değil de toplumsal fayda sağlamak adına gerçekleştiren bu bireyler hacktivistler olarak değerlendirilmekte ve felsefeleri veya eylem biçimleri ise hacktivizm olarak tanımlanmaktadır.

Yukarıda da belirtildiği gibi, hacktivistler eylemlerini toplumsal fayda sağlamak adına gerçekleştirmektedirler. Dolayısıyla, özellikle toplumsal sorumluluklarını yerine getirmeyen veya kamuoyunun tepkisini çeken faaliyetlere girişen firmaların, hacktivistler tarafından hedef alınma olasılıkları oldukça yüksek olarak görülmektedir. Bu açıdan bakıldığında, hacktivist hareketlerin firmalar açısından ne gibi sonuçlar doğuracağını anlayabilmek önem kazanmaktadır.

Özellikle son yıllarda, küreselleşen ekonomideki artan rekabet nedeniyle firmalar sürdürülebilir rekabet avantajı sağlayabilecek yeni yolları aramaya koyulmuş ve gayrı maddi varlıkların incelenmesine de daha çok önem verilmeye başlanmıştır (Schwaiger, 2004: 46; Cravens ve diğerleri, 2003: 202). İtibarın da; nadir, değerli, sürdürülebilir ve taklit edilemez olduğu ve bu sayede rekabet avantajı sağlayabilecek önemli bir gayrı maddi varlık olduğu düşünülmektedir (Schwaiger, 2004: 51).

Gardberg ve Fombrun'a (2002: 303) göre; kurumsal itibar, kurumsal rekabet avantajını sürdürmede giderek daha fazla öneme sahip bir unsur halini almakta ve bu durum; piyasaların küresel olarak iç içe geçmesi, medyadaki tıkanma ve parçalanma, daha konuşkan paydaşların ortaya çıkması ve endüstrilerin ve ürünlerinin metalaştırılmasından kaynaklanmaktadır. Bu akımların firmalar üzerinde yarattığı baskılar firmaları farklılaşmaya zorlamakta ve kurumsal itibar önemli bir stratejik silah olarak öne çıkmaktadır. Shamma'ya (2012: 151) göre, kurumların eylemleri hakkındaki kamusal farkındalığın artması, iletişim biçimlerinin değişmesi, kurumsal

şeffaflığın önem kazanması gibi sebepler de kurumsal itibarın önemini arttırmaktadır.

İyi bir itibarın bir firma için birçok faydası olabilmektedir. İyi bir itibar, firmanın paydaşlarına ürün ve hizmetlerinin ve firmayla yapılacak olan mübadelelerin güvenilir ve beklentileri karşılayacak şekilde olduğuna işaret etmektedir (Cravens ve Oliver, 2006: 296). İyi bir itibar sayesinde; müşterilerin kaliteli ürünler için daha fazla fiyat ödemesi (Roberts ve Dowling, 2002: 1079; Fombrun ve Shanley, 1990: 233), firmanın daha iyi adayları işe alması (Fombrun ve Shanley, 1990: 233), çalışanlarının performanslarının artması (Roberts ve Dowling, 2002: 1079; Gray ve Balmer, 1998: 698), yatırımcıları çekmesi (Fombrun ve Shanley, 1990: 233), sermaye maliyetlerinin düşmesi (Fombrun ve Shanley, 1990: 255) ve rekabet kabiliyetlerinin artması (Roberts ve Dowling, 2002: 1077; Rao, 1994: 29; Fombrun ve Shanley, 1990: 255; Schwaiger, 2004: 47) gibi faydalar sağlanabilmektedir. Olumlu bir kurumsal itibara sahip firmanın herhangi bir birleşme durumunda kendilerine uygun bir firma bulma olasılığı da daha fazladır (Caruana, 1997: 114). Bir firmanın arz ettiklerinin kalitesi konusunda bir belirsizlik olduğunda itibar önemli bir etken olarak devreye girecektir (Roberts ve Dowling, 2002: 1079).

Yukarıdaki açıklamalar ışığında, hacktivist eylemlerin kurumsal itibar açısından ne gibi sonuçlar doğurabileceğinin anlaşılması önem kazanmaktadır. Hacktivist eylemlerin işletmeler açısından pek çok olumlu veya olumsuz sonuca yol açabilme olasılığı bulunsa da, bu çalışmada hacktivizm ve kurumsal itibar arasında nasıl bir bağlantı olduğu sorusuna yanıt aranmaktadır. Dolayısıyla, bu çalışmanın amacı hacktivizm ve kurumsal itibar ilişkisini incelemektir. Bu ilişkiyi açığa çıkarabilmek adına yerli ve yabancı yazın taraması yöntemine başvurulmaktadır. Gerek geliştirilen araştırma modeliyle, gerekse kurumsal itibar ve hacktivizm ilişkisine yönelik bağlantıları ele almasıyla, bu çalışma alan yazında öncül olma niteliği taşımakta ve yazına önemli bir katkı yapmaktadır.

Çalışmanın birinci bölümünde hacktivizm kavramı ele alınmaktadır. Hacktivizm kavramı açıklanırken, hacktivizmle benzer olarak görülen diğer kavramlara da değinilerek hacktivizmin bu kavramlarla olan benzerlikleri ve farklıları açıklanmaktadır. Daha sonra ise, hacktivizmin tarihsel evrimine ilişkin kısa

bir değerlendirmenin ardından alan yazında var olan hacktivizm tipolojileri açıklanmaktadır.

Çalışmanın ikinci bölümünde kurumsal itibar kavramı incelenmektedir. Kurumsal itibarın kavramsal yapısını anlamak adına, öncelikle kurumsal itibar kavramının ne olduğu ve neleri içerdiği ele alınmakta ve alan yazında var olan çeşitli sınıflandırmalara göre kurumsal itibar ekolleri açıklanmaktadır. Bunun ardından, kurumsal itibara yönelik ölçümlere değinilmektedir.

Çalışmanın üçüncü ve son bölümünde ise; PytlikZillig ve arkadaşlarının (2014) hacktivizme destek/direnç modeliyle, Schwaiger'in (2004) kurumsal itibar modelleri bütüncül bir bakış açısıyla ele alınmakta olup, bu modellerden hareketle hacktivizm ve kurumsal itibar ilişkisine yönelik bir araştırma modeli oluşturulmaktadır.

BİRİNCİ BÖLÜM
HACKTİVİZM KAVRAMININ TANIMI, ANLAMI VE DİĞER KAVRAMLARLA İLİŞKİSİ, TARİHSEL GELİŞİMİ VE HACKTİVİZME TİPOLOJİK YAKLAŞIMLAR

1.1. HACKTİVİZM KAVRAMININ TANIMI VE ANLAMI

Hack eylemi ve aktivizmin birlikteliğini temsil eden hacktivizm kavramı (Denning, 2001: 241), son yıllarda özellikle politik arenada sıklıkla tartışılan bir olgu olmasına rağmen, işletme alanında konu üzerine yapılan çalışmalar sınırlı sayıdadır. Yine de hacktivistlerin kar amacı güden kuruluşlara yönelik faaliyetleri, hacktivistlerin bu kurumlara yönelik eylemlerinin nedenlerinin ve sonuçlarının daha yakından incelenmesini bir gereklilik haline getirmektedir.

Hacktivizm kavramı 1996 yılında Cult of the Dead Cow (cDc) grubunun Omega rumuzlu üyesi tarafından ortaya atılmıştır ve hack eylemlerinin politik amaçlar doğrultusunda gerçekleştirilmesi anlamında kullanılmıştır (Ruffin, 2004). Kavram köken olarak hack ve aktivizm kavramlarının birleşiminden doğmaktadır. Dolayısıyla, hacktivizm kavramını anlayabilmek için, öncelikle onu meydana getiren hack ve aktivizm kavramlarını daha yakından ele almak gerekmektedir.

En basit anlamıyla hack; hackerların idealleriyle bütünleştirerek gerçekleştirdikleri eylemleri ifade etmektedir (Jordan ve Taylor, 2004: 9) ve düzenli bir programlama hilesini temsil etmektedir. Bilgisayarlara yasadışı olarak sızmayı çağrıştırsa da, hacker toplulukları tarafından teknolojinin; orijinal, alışılmışın dışında ve yenilikçi bir yolla kullanılması olarak tarif edilmektedir. Dolayısıyla, hack kavramı sadece bilgisayar hileleri ile sınırlı kalmamakta, aynı zamanda teknolojiyle ilgili herhangi bir unsurun yukarıda bahsedilen şekilde asıl amacının dışında kullanılması için geliştirilen hile de hack olarak nitelendirilmektedir. Hack kavramının en temel özellikleri ise; basit olması, uzmanlık gerektirmesi ve yasal olmamasıdır (Jordan ve Taylor, 2004: 6-8). Örneğin; eski tip ankesörlü telefon kulübelerinden sadece 100 kontörlük bir telefon kartı, bir mıknatıs, kaset bandı ve yapıştırıcı yardımıyla sınırsız arama yapabilmek mümkündü. Bu örnek aslında hack kavramını çok iyi özetlemektedir. Öncelikle oldukça basit olması, ancak ankesörlü telefon sistemlerinin işleyiş biçimi hakkında bilgi sahibi olunmasını gerektirmesi ve

buna ek olarak pek yasal sayılamayacak bir eylem olması bakımından hack eyleminin temel özelliklerini oldukça net bir şekilde ortaya koymaktadır. Tabi ki teknoloji geliştikçe eski usuller de işlerliğini yitirmektedir. Nitekim günümüzde, telefon kulübelerinde kullanılan sistemler ve kartlar daha güvenli hale getirilmiştir. Yine de, mevcut sistemleri farklı şekillerde kullanmanın her zaman yeni ve yaratıcı bir yolu bulunabilmektedir.

Tablo 1: Hackerlara Verilen Farklı Etiketler

Kategori	**Tanım**
Siyah Şapkalı Hackerlar	Kötü hackerlar olarak bilinen, kurumların güvenlik sistemlerine teknolojik veya ekonomik zararlar vermeyi amaçlayan kişiler
Beyaz Şapkalı Hackerlar	Siyah şapkalı hackerların zarar verici faaliyetlerini engellemeye çalışan kişiler
Gri Şapkalı Hackerlar	Değişken etik standartları bulunan, zaman zaman siyah şapkalı zaman zamansa beyaz şapkalı hackerlar gibi hareket eden kişiler
Kırıcılar (Crackers)	Çeşitli yazılımların yasal olmayan kopyalarını yapan ve şifre ve kod çözmede uzmanlaşmış kişiler
Script Kiddies	Kendilerine ait hack programları geliştiremeyen ve bu sebeple hali hazırda var olan hack programlarını kullanan kişiler
Phreaks	İletişim teknolojilerini bedava kullanabilmek için bu teknolojileri hackleyen kişiler
Carding	Kredi kartı bilgilerini çalarak hesaplarına para aktarmaya çalışan kişiler
Kriptograflar (Şifre çözücüler)	Genellikle üniversitelerde veya büyük firmalarda çalışan ve karmaşık şifre çözme yazılımları kullanan, hack tekniklerini bilen ancak nadir kullanan kişiler
Siber (Sanal) savaşçılar	Kendi devletleri veya istihbarat teşkilatlarıyla birlikte çalışan, diplomatik sorunlarda ülkeleri adına diğer ülkelerin dijital altyapılarına saldıran kişiler
Hacktivistler	Hackerlar ve aktivistlerin karışımı olan, çeşitli ideolojik amaçları gerçekleştirmek adına hack tekniklerine başvuran kişiler
Spammers	İdeolojik, ticari veya sadece eğlenmek amacıyla sıradan insanlara istenmeyen elektronik email gönderen kişiler

Kaynak: Papadimitriou, 2006: 321.

Hack eylemini gerçekleştirenlere ise; hacker, cracker vb. pek çok farklı etiket verilmektedir. Hacker, cracker, siyah şapkalı hacker, beyaz şapkalı hacker, script

kiddies vb. kavramların ayrımları hacker toplulukları dışında pek fazla yapılmamakta, bu da farklı tip saldırıların hacktivizmle ilişkilendirilmesine neden olmaktadır. Tablo 1'de bu kavramların her birine ait açıklamalar yer almakla birlikte, hacker ve cracker kavramlarına ayrı bir parantez açma gereği duyulmuştur.

Hackerlar, bilgisayar sistemleri ve ağları ile ilgili kavrayışları oldukça ileri düzeyde olan ve bu sistemleri orijinal hallerinden farklı bir amacı gerçekleştirmeleri için becerilerini bu sistemleri yeniden tasarlamak, düzenlemek ve icat etmek için kullanan bireyler olarak tanımlanırken (Chu ve diğerleri, 2009: 2375), crackerlar ise yıkıcı sonuçlar elde etmek için bilgisayar sistemlerine sızan bireyleri nitelendirmektedir (Levesque, 2006: 1203). Her iki kavram da bilgisayarlara yasadışı sızan bireyleri tarif etmek için kullanılmaktayken, hackin temel değerleri olduğunu düşünenler hacker kavramını kullanırken, cracker kavramı ise bilgisayar güvenliği sektöründe olduğu gibi bu değerlere karşı çıkanlar tarafından kullanılmaktadır (Taylor, 2005: 628). Hacker ve cracker kavramları arasındaki bu farklılık hacktivizmin içinde dahi kendini göstermektedir.

Hack kavramı açıklandığına göre, hacktivizm kavramının ikinci ana unsuru olan aktivizm kavramına da kısa bir parantez açmak gerekmektedir. Aktivizm; politik veya toplumsal güdülü eylemler, bildiriler ve hareketler olarak tarif edilebilse de; boykotlar, oturma eylemleri vb. protesto biçimlerinin yasallığı üzerine farklı görüşler, aktivizmi tanımlaması zor bir kavram haline getirmektedir (Beach, 2012: 7). Denning'e (2001: 241) göre aktivizm kavramı; bir gündem veya amaca destek sağlamak adına internetin tahrip edici olmayan bir şekilde kullanılmasını temsil etmektedir. Her ne kadar burada aktivizm internet çağındaki çağrışımıyla ifade edilse de, bahsi geçen gündem veya amaç geçmişten günümüze; insan hakları ihlalleri, küreselleşme, bilginin ticarileşmesi, sömürge anlayışı, kapitalizm vb. pek çok konuda sergilenen aykırı duruşu da temsil etmektedir.

Jordan ve Taylor'a (2004) göre; aktivizm hacktivizmin temelini oluşturan önemli bir öğedir. Bu bağlamda hacktivizmi; aktivizmin bilgi ve teknoloji çağındaki yansıması, bir başka ifadeyle aktivizmin hack eylemleriyle bütünleşerek evrimleşmiş hali olarak da nitelendirebilmek mümkündür. Nitekim Jordan ve Taylor (2004: 1) hacktivizmi; hack eylemleri ve kökleşmiş politik protestoların bir kombinasyonu ve popüler politik eylemlerin sanal aleme taşınmış hali olarak tanımlamaktadır. Bir

başka deyişle hacktivizm; "aktivizmin elektronikleşmiş halini" ve doğrudan eylem biçiminin sanal aleme taşındığı özel bir sosyal ve kültürel olguyu betimlemektedir.

Hacktivizm hack ve aktivizm kavramlarının birleşiminden doğmakta, ancak bu iki kavram farklı çevreler tarafından farklı şekillerde yorumlanabilmektedir. Bu durum da çoğunlukla hacktivizmle alakası olmayan sanal saldırıların da hacktivizm olarak yansıtılmasına neden olmakta ve kavramla ilgili karmaşa yaratmaktadır. Nitekim Krapp'ın da belirttiği üzere (2005: 73), hacktivizm bazıları tarafından elektronik doğrudan müdahaleler vasıtasıyla sosyal değişim yaratma yolu olarak görülürken, bazıları tarafından ise internet üzerinden gerçekleştirilen zarar verici eylemler olarak yorumlanmakta ve bu sebeple oldukça tartışmalı bir olgu olarak nitelendirilmektedir. Benzer şekilde metac0m (2003) hacktivizmin farklı şekillerde yorumlandığına değinmekte, bu nedenle de hacktivizm kavramını tanımlamaktansa, ruhunu tarif etmenin daha doğru olduğunu savunmakta ve hacktivizmi sürekli olarak evrimleşen, açık kodlu, kimsenin tekelinde olmayan bir süreç olarak tarif etmektedir.

Vegh (2003: 83) hacktivizmi; "devlet dışı aktörler tarafından hoşnutsuzluklarını vurgulamak için misilleme yapmak veya aktivistler tarafından savunulan bir konuya dikkat çekmek için yapılan politik güdülü tek olaylık online (çevrimiçi) eylem veya kampanya" olarak tanımlamakta ve bakış açılarının farklılığı sebebiyle kavramın; çevrimiçi avukatlık, sanal doğrudan eylem, elektronik sivil itaatsizlik, performans sanatı, sanal suç, sanal terörizm ve sanal savaş gibi farklı etiketler aldığını belirtmektedir. Dolayısıyla, hacktivizmi daha iyi anlayabilmek için hacktivizm ve onunla sıklıkla karıştırılan kavramların farklarını ortaya koymak önem kazanmaktadır.

1.2. HACKTİVİZM KAVRAMININ DİĞER KAVRAMLARLA İLİŞKİSİ

1.2.1. Hacktivizm ve Elektronik Sivil İtaatsizlik

Elektronik sivil itaatsizlik; boykotlar, sokak gösterileri ve oturma eylemleri gibi geleneksel protesto biçimlerinin sanal alem için yeniden yaratılması olarak tanımlanmaktadır (Jordan ve Taylor, 2004: 3). Ancak bu protesto biçimleri hacktivistler tarafından da sıklıkla kullanıldığına göre hacktivizm ve elektronik sivil itaatsizlik arasındaki çizginin nerede ayrıldığı sorusu önem kazanmaktadır.

Hacktivizim ve elektronik sivil itaatsizlik kavramı arasındaki karmaşanın

temel sebebi, Samuel'in (2004) de değindiği gibi hacktivistlerin her zaman kendilerini hacktivist olarak tanımlamaması gibi görünmektedir. Örneğin Critical Art Ensemble (CAE) adlı aktivist oluşumdan doğan Electronic Disturbance Theatre (EDT) adlı erken dönem hacktivist oluşumlardan biri olarak görülen grup, eylemlerini sıklıkla elektronik sivil itaatsizlik olarak nitelendirmekteyken, ilgili alan yazında ise bu grubun hacktivist bir oluşum olduğu üzerine bir fikir birliği olduğu açıkça görülmektedir. O halde, elektronik sivil itaatsizliğin aslında hacktivizmin eylem biçimlerinden sadece bir kısmını yansıttığını, dolayısıyla hacktivizmin bir parçasını temsil ettiğini ancak bütününü ifade etmediğini iddia edebilmek mümkündür. Bir başka değişle, hacktivizm elektronik sivil itaatsizliğe kıyasla daha geniş bir anlamı ifade etmektedir. Nitekim Denning (2001: 263) de hacktivizmin, sivil itaatsizlik yöntemlerini sanal aleme taşıyan elektronik sivil itaatsizliği kapsadığını belirtmektedir.

Bu iki kavramın zaman zaman benzer olarak görülmesi, ilk hacktivist oluşumların sanal oturma eylemleri gibi elektronik sivil itaatsizliğin ana eylem biçimlerinden biri olan yöntemleri kullanmalarından kaynaklanmaktadır. Buna ek olarak bazı hacktivist eylemlerin temeli, sivil itaatsizliğin anlayışlarına ve onun temel prensiplerine dayanmaktadır. Blodgett'a (2009: 137) göre; politik değişim sağlama aracı olarak hacktivizm, bir yöntem olarak sivil itaatsizliğin anlayışlarından yararlanmakta ve politik kontrol ve baskı kurabilmek için yeni taktik inovasyonlar kullanarak, belirli bir politik bağlam üzerinde kontrol sağlamada yeni yollar yaratmak için de kullanılmaktadır. Sivil itaatsizliğin anlayışları ve temel prensipleri, eylemlerin; kişiye veya mülke zarar vermemesi, şiddet içermemesi, kişisel kazanç amaçlı olmaması, etik güdülere (bir yasanın adil olmadığını veya kamu yararına olmadığını düşünmek gibi) dayanması ve eylemlerin sonuçlarından doğacak kişisel sorumluluğun gönüllü olarak kabul edilmesi olarak ele alınmaktadır (Manion ve Goodrum, 2000: 15). Dolayısıyla hacktivizm ve elektronik sivil itaatsizlik arasındaki karmaşanın temel sebebi hacktivizmin ilk yıllarında elektronik sivil itaatsizlikle olan benzerliğidir.

1.2.2. Hacktivizm ve Sanal Terörizm

Bazı medya kanallarında sıklıkla hükümetlere yönelik sabotaj, yıkım ve faaliyetleri aksatmaya yönelik hareketler olarak yansıtılan hacktivizm, aslında daha çok özgürlüğe dikkat çeken, insan hakları ihlallerine değinen ve bilginin serbest dolaşımını savunan, daha açık bir ifadeyle çağımızda demokrasi kavramıyla birbirine yapışan bir harekettir (Fitri, 2011: 2). Hacktivizm her ne kadar medyada sıklıkla sanal terörizm gibi yansıtılsa da ondan farklıdır (Kenney, 2015: 118). Sanal alem ve terörizmin birleşimini temsil eden sanal terörizm kavramı; terörizm kavramının sanal karşılığıdır. Can kaybına neden olmak veya ciddi ekonomik zararlar vermek gibi niyetlerle gerçekleştirilen politik güdümlü, ağır hasarlara yol açan hack eylemlerini kapsamaktadır. Örneğin hava kontrol sistemlerine girerek uçakları çarpıştırmak bu tip bir eylem örneğidir (Denning, 2001: 241). Öte yandan, hacktivistler iyi bir sebepleri olmadıkça saldırmamakta ve saldırıları genellikle bir zarar vermekten ziyade hedefteki kişi veya kurumdan duyulan hoşnutsuzluğu gösteren açık bir mesaj vermek için yapılmaktadır. (Papadimitriou, 2009: 1332). Bilgi birikimlerini ve yazılım araçlarını kullanarak gerçekleştirdikleri eylemlerden maddesel kazanç sağlamayı veya geniş çaplı bir yıkım yaratmayı değil, hedeflerine yönelik saldırılarını kamuya etkili bir şekilde duyurarak kamuoyunun dikkatini çekmeyi amaçlamaktadırlar (Kenney, 2015: 117-118). Bu bağlamda, sanal terörizmi hacktivizmden farklılaştıran, saldırıların basitçe mağdurları rahatsız etmesinden öteye geçerek, onlara, mülklerine veya kritik alt yapılara ciddi zarar verebilecek eylemleri temsil etmesidir (Kenney, 2015: 122). Dolayısıyla hacktivizm ve sanal terörizm arasındaki temel fark hacktivizmin korku ve terör yaratma amacı taşımamasıdır (Holt, 2012: 340).

Aktivizm, hacktivizm ve sanal terörizm birbirlerinden farklı kavramlar olmakla birlikte, hacktivizm diğer iki eylem biçimi arasındaki bir ara form olarak da algılanmaktadır. Denning'e (2001: 241-242) göre; aktivizmden sanal terörizme doğru gidildikçe verilen hasar artmakta ancak bu durum verilen zararın büyüklüğünün politikaya aynı derece etki edeceği anlamına gelmemektedir. Örneğin; bir milyon imzalı bir elektronik dilekçe, acil servis hizmetlerine yönelik bir saldırıya kıyasla politikayı daha fazla etkileyebilmektedir. Bu üç eylem türü birbirlerinden farklı olarak değerlendirilse de; herhangi bir bireyin sadece aktivist, sadece hacktivist veya

sadece sanal terörist olduğu anlamına gelmemektedir. Bu durum yapılan eylemin türüne ve diğerlerinin eyleme yönelik algısına göre de şekillenmektedir. Hacktivizm ve sanal terörizm söz konusu olduğunda ise; bunlara benzer eylemleri gerçekleştiren grupların dış siyaset üzerinde etkili olma olasılığı, tahribata yönelik eylemler gerçekleştiren grupların dış siyaset üzerinde etkili olma olasılığından daha düşüktür. Hükümete ait bilgisayarları kontrol edebilmeleri ve medyanın dikkatini çekebilmeleri, güçlendirme hissine kapılmalarını sağlayabilmekte fakat bu siyasi kararları değiştirebilecekleri anlamına gelmemektedir. Burada ortaya çıkan asıl etki, aktörlerin taleplerinin karşılanmasından ziyade, ulusal ve uluslararası sanal savunma politikalarının güçlendirilmesidir.

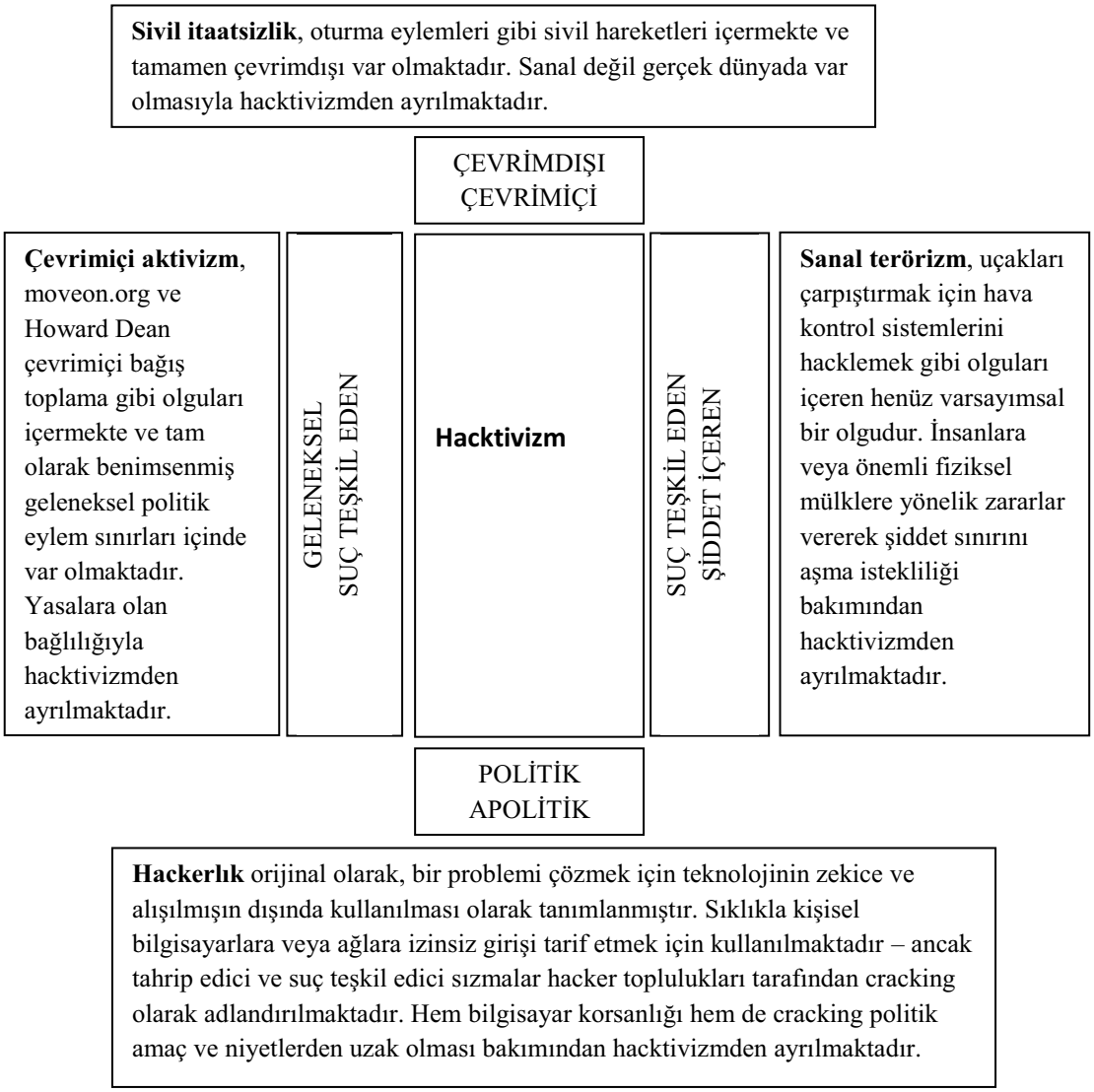
1.2.3. Hacktivizm ve Çevrimiçi Aktivizm

Hacktivizmle karıştırılan bir diğer kavram ise çevrimiçi aktivizmdir. Çevrimiçi aktivizm; "internete dayanan politik güdülü bir hareket" olarak tanımlanmaktadır (Vegh, 2003: 71). Araştırmacıların kavramlara yönelik farklı bakış açıları bu kavramların zaman zaman iç içe geçmesine neden olmaktadır. Örneğin Vegh (2003), çevrimiçi aktivizmin; farkındalık/savunuculuk, örgütlülük/mobilizasyon ve etki/tepki olmak üzere 3 farklı formda ortaya çıktığını ve hacktivizmin çevrimiçi aktivizmin etki/tepki sınıfında yer aldığını savunmaktadır. Bu bakış açısına göre çevrimiçi aktivizm hacktivizmi kapsamaktadır. Benzer şekilde Yang (2009: 34), çevrimiçi aktivizm eylemlerini ele alırken web sitelerinin hacklenmesini çevrimiçi aktivizmin en radikal türü olarak değerlendirmekte, çevrimiçi dilekçeler veya yürütülen kampanyalarla ilgili web siteleri kurmayı ise çevrimiçi aktivizmin yaygın yöntemleri olarak ele almaktadır. Milone (2003: 77) ise hacktivizmi tanımlarken, çevrimiçi aktivizmden yola çıkmakta ve çevrimiçi aktivizmin bilgisayarlara gizlice sızıldığı veya potansiyel olarak zararlı yazılımlar kullanılarak gerçekleştirildiği durumlarda hacktivizm olarak adlandırıldığını belirtmektedir. Öte yandan Samuel'e (2004: 4) göre, çevrimiçi aktivizm ve hacktivizm birbirlerinden farklı kavramlar olmakla birlikte aralarında önemli sınırlar bulunmaktadır.

Hacktivizmi; "politik sonuçlar elde etmek adına, yasal olmayan veya yasallığı muğlak dijital araçların şiddet içermeyen bir şekilde kullanılması" olarak

tanımlayan Samuel (2004: 2); hacktivizmi sadece çevrimiçi aktivizmden değil, sanal terörizm, hacker ve sivil itaatsizlik kavramlarından da ayrımlaştırma gereğini duymuştur. Samuel yaptığı bu tanımla, kavramı benzer kavramlardan gözle görülür şekilde farklılaştırmaktadır. İlk olarak, şiddet içermemesi onu sanal terörizmden farklılaştırmaktadır. İkinci olarak hacktivizmin yasal olmayan veya yasallığı muğlak eylemleri, onu suç teşkil etmeyen eylemlerin gerçekleştirildiği çevrimiçi aktivizmden ayırmaktadır. Üçüncü olarak ise; şiddet içermeyen ancak suç teşkil eden dijital araçların kullanımına değinerek, önemli bir ayrımı göstermektedir (Samuel, 2004: 3). Şekil I'de Samuel'e (2004) göre hacktivizm ve diğer kavramlar arasındaki önemli sınırlar ve farklılıklar resmedilmektedir.

Şekil 1: Hacktivizmin Sınırları



Kaynak: Samuel, 2004: 4.

Şekil I'e göre hacktivizm ve geleneksel hack eylemleri arasındaki temel farklılık hacktivist hareketlerin politik, geleneksel hack eylemlerinin ise apolitik olmasından kaynaklanmaktadır. Hacktivist eylemlerin suç teşkil etmesi ise onu yasal protestoları çevrimiçi platforma yansıtan çevrimiçi aktivizmden ayırmaktadır. Ancak yapılan hacktivist eylemlerin suç teşkil etse de şiddet içermemesi, hacktivizmi şiddet içeren eylemlerin gerçekleştirildiği sanal terörizmden farklılaştırmaktadır. Son olarak ise hacktivizm çevrimiçi bir hareket olarak ele alınmakta ve bu yönüyle çevrimdışı olan sivil itaatsizlikten ayrılmaktadır.

1.2.4. Hacktivizm, Sanal Saldırı ve Sanal Savaş

Hacktivizm yukardaki kavramlara ek olarak sanal saldırı ve sanal savaş kavramlarıyla da sıklıkla karıştırılmaktadır. Ancak Kenney'in (2015) de ele aldığı üzere sanal saldırı, sanal savaş ve hacktivizm kavramları arasında önemli farklılıklar bulunmaktadır. Kenney'e (2015: 112) göre; sanal saldırı, sanal savaş, hacktivizm ve sanal terörizm eylem biçimleri açısından metaforik olarak aynı familyada yer almakta ve bu sebeple her familyadaki farklı türlerde görüleceği üzere aralarında önemli benzerlikler olsa da, aynı zamanda önemli farklılıklar da bulunmaktadır. Sanal savaş, düşmanların sanal altyapısını bozmaya veya düşmanların sanal saldırılar gerçekleştirmesini engellemeye yönelik saldırgan bilgisayar taarruzlarını temsil etmektedir (Kenney, 2015: 114). Sanal saldırı ise; "bilgisayar sistemlerini, ağlarını veya bu sistemler ve/veya ağlardaki bilgi ve programları kasti olarak değiştirme, bozma, aldatma, parçalama veya yok etme eylemlerini temsil etmektedir" (Lin ve diğerleri, 2009: 1). Bu bağlamda, sanal saldırı kavramını diğerlerinden ayıran temel noktalar; eylemin yıkıcı olmasa da düşmanca bir niyetle gerçekleştirilmesi, eyleme girişen aktörler (devlet veya devlet dışı), eylemin yol açabileceği zararın çapı (aşırı veya minimum) ve hangi motivasyonla yapıldığı (politik, ekonomik, sosyal veya psikolojik) gibi konulardaki çeşitliliktir. Sanal savaş kavramı ise; aktörlerinin devletler veya ulusal çıkarları korumaya yönelik onlar adına hareket ettiğine inanan asker (private) hackerlar olması bakımından diğer kavramlardan ayrılmaktadır (Kenney, 2015: 113-114).

Hacktivizm ve sanal savaş kavramları arasındaki farkın daha iyi anlaşılabilmesi adına hacktivistlerin sanal savaş konusundaki tutumuna da değinmek

üzere yaşanmış bir örnekten yola çıkmak faydalı olacaktır. Aralık 1998'de IRC sohbet üzerinde yapılan bir basın konferansı sırasında Legion of the Underground (LoU) adlı gruba üye olan bir hacker Çin'deki ve Irak'taki insan hakları ihlallerini gerekçe göstererek bu ülkelerin bilgisayar sistemlerinin tamamının çökertilmesi amacıyla sanal savaş ilanında bulunmuştur. Buna karşın, pek çok hacktivist oluşum bu çağrıya karşı çıkarak bunun hacktivizm etiğine uymadığını belirtmiştir. Nitekim 7 Ocak 1999'da; Chaos Computer Club, the Cult of the Dead Cow, !Hispahak, L0pht Heavy Industries, Phrack, Pulhas ve Dutch hacking community adlı oluşumlardan toplamda 2600 kişi, bir ülkeye karşı savaş ilan etmenin bir hacker grubunun yapabileceği en sorumsuz davranış olduğunu belirten bir mektuba imza atarak, bunun hacktivizme aykırı olduğunu belirtmişlerdir. Bu paktın hemen ardından LoU da; bir üyelerinin yaptığı savaş ilanının grubun pozisyonunu temsil etmediğine yönelik bir bildiri yayınlamıştır (Denning, 2001: 275-276). Bu örnekten yola çıkarak, en azından hacktivist topluluklar arasında sanal savaşın hacktivizme benzemediği ve hatta birbirleriyle hiçbir bağının olmaması gerektiğine dair bir inanç olduğunu söyleyebilmek mümkündür.

1.2.5. Hacktivizm ve Sanal Casusluk

Son olarak ise; sanal casusluk kavramına kısaca değinerek hacktivizmden neden farklı olduğunu açıklamak faydalı olacaktır. Sanal casusluk en basit tabirle; "genellikle bir hükümete veya bir örgüte ait gizli bilgilerin bilgisayar ağlarına yasadışı girişler vasıtasıyla elde edilmesi" olarak tanımlanmaktadır (www.oxforddictionaries.com). Sanal casusluk kavramındaki anahtar nokta gizli bilgilerin rekabet avantajı veya finansal kazanç sağlamak için ele geçirilmek istenmesidir. Öte yandan, hacktivizm söz konusu olduğunda asıl amaç finansal kazanç veya rekabet avantajı elde etmek değil, protesto edilen hususun gündeme gelmesini ve dikkat çekmesini sağlamaktır (Beach, 2012: 14). Dolayısıyla bu iki kavram birbirlerinden tamamıyla farklıdır.

Bölüm boyunca yapılan açıklamalardan yola çıkarak hacktivizmin belli başlı kabul gören özellikleri olduğunu öne sürebilmek mümkündür. Bu özellikleri aşağıdaki şekilde sıralayabilmek mümkündür:

- Eylemlerin şiddet içermemesi,

- Bireysel kazanç adına değil kamu yararına yapılması (veya eylemi gerçekleştirenlerin gerçek niyetlerinin bu yönde olması),
- Kamuoyunda protesto edilen konu hakkında farkındalık yaratmanın amaçlanması,
- Hack tekniklerinin kullanılması.

O halde hacktivizmi; "belirli bir gündem veya amaç doğrultusunda, kamuoyunda farkındalık yaratmak amacıyla ve bireysel kazanç elde etmek adına değil kamu yararına olacağı inancıyla, hack tekniklerinin şiddet içermeyecek şekilde kullanılması" olarak tanımlayabilmek mümkündür.

1.3. HACKTİVİZMİN TARİHSEL GELİŞİMİ

Hack ve aktivizm gibi iki kök kavramı bünyesinde barındıran hacktivizmin tarihsel evrimini, köklerinden bağımsız olarak açıklayabilmek pek mümkün gözükmemektedir. Daha açık bir ifadeyle, hacktivizmin nasıl evrimleştiğini anlayabilmek için hem aktivizmin hem de hackerlığın evrimini ele almak gerekmektedir.

Hacktivizm; hack, bilgi toplumları ve modern sosyal protesto veya direniş gibi üç farklı akımın kesişiminden doğmuştur (Jordan ve Taylor, 2004: 2). Her ne kadar bu kesişim 1990'lı yılların ortalarından itibaren hacktivizmin bir eylem biçimi olarak ortaya çıkmasını sağlamış olsa da, tarihsel olarak bakıldığında köklerinin 1960'lı yıllarda ABD'deki MIT üniversitesinde atıldığını öne sürebilmek mümkündür.

Hack kavramı MIT öğrencilerinin kendi aralarında yaptıkları eşek şakalarına (pranks) verdikleri bir isim olarak bilinmekteyken, Tech Model Railroad Club adlı öğrenci klübünün üyeleri kavramı farklı bir anlamı ifade edecek şekilde kullanmaktaydı. Klüp üyeleri model demiryolu ağı üzerinde yaptıkları etkili ve basit düzenlemelerle sistemin daha iyi işlemesini sağladıklarında topluluk üyeleri bu düzenlemeleri hack olarak tarif etmekteydi (Akdeniz, 2013: 9-10). Dolayısıyla hack kavramı bu sayede zamanla eşek şakası anlamına gelen ilk anlamını yitirerek, teknolojiyi yeni ve basit bir yolla yeniden tasarlamak anlamına gelen ikinci anlamıyla kullanılmaya başlamış ve hack eylemini gerçekleştiren bireyler topluluk üyeleri tarafından bir saygı göstergesi olarak hacker olarak adlandırılmıştır.

Hackerlık ilk ortaya çıktığı yıllardan itibaren evrimleşerek farklı hacker kuşaklarının ortaya çıkmasına neden olmuştur. Jordan ve Taylor'a (2004; 9-12) göre; teknolojinin gelişmesiyle birlikte ortaya çıkan yedi farklı hacker kuşağı bulunmaktadır ve hacktivistler bu kuşakların sonuncusudur. Yine de bu durum bir hackerın sadece tek bir kuşağa ait olduğu anlamına gelmemektedir. Bu kuşaklar aşağıda kısaca açıklanmaktadır:

1.Orijinal hackerlar; MIT gibi çeşitli ABD üniversitelerinde merkezi bilgisayarın ilk ortaya çıktığı 1950 ve 1960'lı yıllarda, bu alandaki araştırmaları takip eden öncü kuşaktır.

2.Donanım hackerları; 1970'li yıllarda ilk kişisel bilgisayarların üretilmesinde önemli rol oynayan ve aynı zamanda bilgisayar mucitleri olarak da nitelendirilen kuşaktır.

3.Yazılım hackerları; donanım hackerları tarafından geliştirilen bilgisayarları yarattıkları programlarla evrimleştiren kuşaktır.

4.Hackerlar / Crackerlar; 1980'lerin ortalarında ortaya çıkan, bilgisayarlara yasadışı yollarla sızan kuşaktır. Ancak amaç her zaman sistemlere zarar vermek değildir. Hacker toplulukları dışındaki gruplar bu eylemleri gerçekleştirenlerin hepsini hacker olarak görmekte ve bu kavramı bilgisayar suçu işleyen kişileri tanımlamak için kullanmaktadır. Hacker toplulukları ise zararlı amaçlarla bu eylemleri gerçekleştirenleri cracker olarak nitelendirmekte ve bunun hacker kavramından farklı olduğunu belirtmektedir.

5.Microserferlar; Microsoft gibi büyük firmalarla işbirliği yaparak onlar için programlar geliştiren kuşaktır. Aynı zamanda elektronik burjuva olarak adlandırılan sınıfın önemli bir bölümünü oluşturmaktadırlar.

6.Açık kaynak; yazılımların ticari amaçtan uzak olması ve açık kodlu olarak yayınlanarak diğerlerinin de en iyi yazılımların geliştirilmesi için katkıda bulunması gerektiğine inanan hackerların kuşağıdır. Buna verilebilecek en güzel örnek, Microsoft'un Windows işletim sistemi gibi ticari yazılımlara karşı geliştirilen Linux işletim sistemidir.

7.Hacktvistler; 1990'lı yılların ortalarından itibaren başlayan, bilgisayar korsanlığı eylemlerini politik duruşlarını aleni bir şekilde göstermek için gerçekleştiren hackerların kuşağıdır.

Hackerlığın evrimini ele alırken, hacker etiğinden de kısaca bahsetmekte yarar vardır. Steven Levy tarafından 1984 yılında yayınlanan "Hackers: Heroes of the Computer Revolution" adlı eser hack tarihinde önemli bir dönüm noktası olmuştur. Özellikle açık kaynak ve hacktivistler gibi son hacker kuşakları, Steven Levy'nin bu eserinde ortaya attığı hacker etiği ilkelerinden önemli ölçüde etkilenmişlerdir. Hacker etiği hackerların belirli etik ilkelere göre hareket etmeleri gerektiğini savunmakta ve bu ilkeler şöyle sıralanmaktadır (Levy, 2010: 23-31):

- Bilgisayarlara ve size dünyanın nasıl işlediğine dair bir şeyler öğretebilecek herhangi bir şeye erişim sınırsız olmalıdır,
- Tüm bilgi serbest olmalıdır,
- Otoriteye güvenilmemeli, ademi merkezileşme desteklenmelidir,
- Hackerlar; derece, yaş, ırk veya pozisyon gibi sahte kriterlere göre değil gerçekleştirdikleri hack eylemlerine göre değerlendirilmelidir,
- Bilgisayar üzerinde sanat ve güzellik yaratmak mümkündür,
- Bilgisayarlar hayatınızı daha iyiye dönüştürebilir,

Hacktivizmin evrimindeki ikinci önemli husus ise aktivist hareketlerin dünya genelinde yaşanan değişimlere paralel olarak evrimleşmesidir. Jordan ve Taylor'a (2004: 41- 66) göre; 1970'li yıllardan önce aktivistlerin mücadele ettiği alanlar genellikle feminist hareketler, kölelik karşıtlığı ve işçi sınıfı hareketleriyken, 1970'li yıllarda bunlara ekolojik mücadele, eşcinselliğin tanınması gibi alanlar eklenirken, 1980'lerde hem soğuk savaş geriliminin artması hem de refah devletinden özelleştirilmiş devletlere geçiş nedeniyle barış ve nükleer karşıtlığı, 1990'larda ise soğuk savaş kaygılarının sona ermesiyle birlikte ekoloji hareketleri ağırlık kazanmaya başlamış ve özellikle şirketlerin çevreye verdiği zararlara yönelik eylemler ve bunu takiben artan küreselleşme ve küreselleşmenin yarattığı köle işçiliğe (farklı ülkelerde düşük ücretle işçilerin çalıştırılması) karşı hareketlere ek olarak, 1990'ların ortalarına doğru Dünya Ticaret Örgütü (DTÖ) gibi küresel örgütlere yönelik küreselleşme karşıtı hareketler ağırlık kazanmaya başlamıştır. 1990'larda artan terör korkusu 11 Eylül 2001'de ikiz kulelere yönelik saldırının ardından iyice tırmanmış ve özellikle ABD'nin Irak işgali gibi terör kaygısı öne sürülerek gerçekleştirilen savaşlara yönelik protestolar ağırlık kazanmaya başlamıştır.

Yukarıda sözü edilen protesto ve hareketlerin hack eylemleriyle kesiştiği noktalar hacktivizmi temsil etmektedir. Dolayısıyla her ne kadar hacktivizm 1996 yılında ortaya atılan bir kavram olsa da, kavram icat edilmeden bile hacktivizmin örneklerini görebilmek mümkündür (Jordan, 2002: 120). Örneğin; Mayıs 1971'de kurulan Youth International Party Line (YIPL) adlı bir yer altı gazetesinin Vietnam savaşı sebebiyle ABD'nin telefon faturalarına getirdiği ekstra vergileri protesto etmek amacıyla takipçilerine telefonlarını hackleyerek bedava konuşabilmenin yollarını göstermesi, hacktivizmin ilk örneği gibi görünmektedir (Jordan ve Taylor, 2004: 13-14). Benzer şekilde, 1989 yılında NASA ağındaki bilgisayarlara yönelik bir saldırı gerçekleştirilmiş ve ağa bağlı bilgisayarların işlem göremez hale gelmesine neden olmuştur. Saldırı ise NASA'nın uzaya gönderdiği uzay araçlarının potansiyel nükleer bombalar olduğu düşünülerek, bunu protesto etmek amacıyla yapılmıştır. (Jordan, 2002: 119-120). Dolayısıyla hacktivizmin tarihsel evrimini ele alırken, başlangıç noktası olarak kavramın ortaya çıkış tarihini değil, hacktivizmde kilometre taşları olarak görülebilecek noktaları ele almak daha doğru olacaktır. Tablo 2'de bu kilometre taşları kronolojik olarak verilmekte ancak tabloda ele alınan olaylar çalışma boyunca detaylı olarak ele alınacağından tekrara girmemesi açısından sadece kısaca açıklanmaktadır.

EDT, Electrohippies, cDc gibi ilk hacktivist oluşumlar çoğunlukla sanal oturma eylemleri, sansüre karşı yazılımlar gibi yasal olarak pek fazla sorunlu görünmeyen eylemler gerçekleştirdiklerinden, çoğunlukla kimliklerini gizleme gereği duymamışlardır. Ancak ilerleyen yıllarda hacktivizmin kapsamı giderek genişlemiş ve web site tahribatları, kamu ve özel kuruluşlara ait bilgilerin ele geçirilerek (bireysel çıkar amaçlı olmamak kaydıyla) kamuoyuyla paylaşılması gibi eylemler ağırlık kazanmaya başlamış ve bu eylemleri gerçekleştirenler kimliklerini gizli tutma gereği duymuşlardır. Hacktivist hareketlerdeki bu değişimin temel sebebi ise Vegh'in (2003) etki tepki olarak dile getirdiği gibi kamu ve özel kuruluşların davranışlarındaki değişim olarak görülebilmektedir. Özellikle devletlerin çevrimiçi gözetim ve sansüre yönelik artan uygulamaları ve hem kamu hem de özel kuruluşlardaki yozlaşma kaygılarının artık toplum tarafından daha ciddi bir şekilde takip edilmesi gibi nedenler, hacktivistlerin eylemlerinin değişiminde önemli rol oynamış gibi görünmektedir.

Tablo 2: Hacktivizmin Evrimindeki Önemli Olaylar

Tarih	Olay
1960-1970	MIT Tech Model RailRoad Club üyelerinin hack kavramına bugünkü anlamını kazandırmaları
1971	Yippies olarak bilinen aktivist hareketin takipçilerine Vietnam savaşı gerekçe gösterilerek telefon faturalarına eklenen vergiyi protesto etmek amacıyla ücretsiz telefon görüşmeleri yapabilmenin yollarını göstermeleri
1981	Chaos Computer Club adlı hacker topluluğunun Berlin'de kurulması
1984	Steven Levy'nin hacker etiğini ortaya attığı devrim yaratan "Hackers: Heroes of the Computer Revolution" adlı eserinin yayınlanması
1986	Mentor olarak bilinen Loyd Blankenship'in Hacker Manifestosunu yayınlaması
1989	WANK (Worms Against Nuclear Killers) olarak bilinen solucanın NASA bilgisayarlarını işlevsiz hale getirmesi
1994	San Francisco merkezli Zippies olarak bilinen bir grubun, açıkhava konserlerini yasaklayan bir yasa çıkarılması sebebiyle, İngiltere hükümetinin sunucularına yönelik DDoS ve e-posta bombardımanı saldırıları gerçekleştirmesi
1995	Fransa'nın nükleer testlerini protesto etmek amacıyla Strano Network adlı grubun hükümet sitelerine yönelik gerçekleştirdiği sanal oturma eylemi
1996	Hacktivizm kavramının Cult of the DeadCow grubunun Omega rumuzlu üyesi tarafından ortaya atılması
1996	John Perry Barlow'un sanal alemin özgürlüğü üzerine bir bildiri yayınlaması
1997	UrBan Ka0s adlı Portekizli bir hacker grubunun Doğu Timor bağımsızlık hareketlerine destek amaçlı olarak, Hindistan hükümetinin web sitelerini hacklemesi
1998	Electronic Disturbance Theatre adlı hacktivist oluşumun Zapatistalara destek vermek adına ABD ve Meksika hükümetlerine ve bazı ticari kuruluşlara yönelik gerçekleştirdikleri sanal oturma eylemleri
1999	Toywar olarak bilinen, Etoys'a karşı yürütülen kampanya
1999	Electrohippies Collective adlı hacktivist oluşumun Seattle'da düzenlenen DTÖ buluşmasını protesto etmek amacıyla düzenlediği sanal oturma eylemleri
2001	Lufthansa uçaklarının kaçak göçmenlerin Almanya'dan sınırdışı edilmesi için kullanılmasını protesto etmek amacıyla, şirketin web sitelerini işlemez hale getirmek için e posta bombardımanına tutulmasına yönelik eylemler
2003	4chan adlı sanal paylaşım platformunun kurulması
2006	Kökleri 4chan'e dayanan Anoynmous'un sosyal ağlarda siyahi avatarların azlığını protesto etmek amacıyla Büyük Habbo Baskını olarak bilinen ilk eylemini gerçekleştirmesi
2008	Anonymous'un Scientology kilisesine karşı gerçekleştirdiği Chanology projesi
2010	Özelllikle Wikileaks hesaplarının PayPal, MasterCard vb. şirketler tarafından kapatılmasıyla birlikte Anonymous'un bu hedeflere yönelik gerçekleştirdiği Operation Payback projesi

Kaynak: Paget'den (2012) uyarlanarak geliştirilmiştir.

Bahsi geçen gruplar ve eylemleriyle ilgili örneklere çalışma boyunca sıklıkla yer verileceğinden, tekrara girmemek adına bu bölümde kısaca açıklanmaya

çalışılmıştır. Dolayısıyla kısa bir özet yapılacak olursa, hacktivizmin ilk ortaya çıktığı zamanlarda insan haklarını ve mahremiyeti korumak için yazılımların geliştirilmesi ve kullanılması olarak değerlendirilirken, ilerleyen zamanlarda internetin ötesinde teknoloji destekli politik aktivizm şeklinde daha geniş bir anlam kazandığını öne sürebilmek mümkündür (Cammaerts, 2013: 427).

Son yıllarda ise yaşanan ekonomik krizler, kamu ve özel kuruluşların yönetiminde şeffaflığın ve etik bilincin önemli olduğu ve kurumların sıradan insanlardan kurumla ilgili bilgileri saklamamaları yönünde bir görüşün giderek ağırlık kazanmasına neden olmuştur (Kaulingfreks F. ve Kaulingfreks R., 2013: 417). Bilginin özgür olması gerektiği inancı son yıllarda giderek daha fazla yaygınlık kazanmakta (Beyer, 2014: 141) ve dolayısıyla, özellikle Anonymous gibi bilginin özgür olması gerektiğine inanan grupların daha fazla destek görmesine neden olmaktadır.

1.4. HACKTİVİZME YÖNELİK TİPOLOJİK YAKLAŞIMLAR

Hacktivizm olgusu tek bir türde ortaya çıkmamakta, hacktivistlerin farklı eylem biçimleri, farklı kökenleri ve farklı yönelimleri gibi sebeplerle çeşitli formlarda görülmektedir. Yine de, alan yazında hacktivizmin farklı formları üzerinde pek fazla durulmadığını söyleyebilmek mümkündür. Nitekim bu bölümde, hacktivizm formlarını ele alan Samuel (2004) ve Jordan ve Taylor'ın (2004) sınıflandırmalarına yer verilecektir.

Samuel'e (2004) göre hacktivizm; hacktivistlerin kökenleri ve yasal yönelimleri göz önünde bulundurulduğunda; politik kırıcılar (political cracking), edimsel hacktivizm (performative hacktivism) ve politik kodlama (political coding) olmak üzere üç farklı tipte görülmektedir. Jordan ve Taylor (2004) ise hacktivizmi; kitlesel eylem hacktivizmi ve dijital doğruculuk hacktivizmi olarak ikiye ayırmaktadır. Kitlesel eylem hacktivizmiyle kastedilen, küreselleşme karşıtlığı gibi olguları bünyesinde barındıran hacktivizm türüdür ki, bu aynı zamanda Samuel'in sanatçı-aktivist kökenden geldiğini savunduğu hacktivistlerin görüşleriyle örtüşmektedir. Dijital doğruculuk hacktivizmi olarak adlandırılan hacktivizm tipi ise; hack eylemlerin doğası gereği olan politik duruşundan kaynaklı hacktivizm tipini betimlemekte ve bu betimleme de yine Samuel'in hacker-programcı kökenden

geldiğini savunduğu hackerların bilginin özgür olması ve paylaşılması gibi görüşleriyle örtüşmektedir. Ancak bu iki sınıflandırma arasındaki temel fark, Jordan ve Taylor'ın (2004) ayrımında hacktivistlerin odak noktalarından ve temel kaygılarından - bir başka değişle kökenlerinden - yola çıkılmasıyken, Samuel'in sınıflandırmasında buna ek olarak hacktivistlerin yasal yönelimlerinin de denkleme katılmasıdır. Hacktivizm tiplerini daha iyi anlayabilmek adına, aşağıda bu farklı sınıflandırmalar ayrıntılı olarak ele alınmaktadır.

1.4.1. Samuel'in (2004) Hacktivizme Tipolojik Yaklaşımı

Hacktivist oluşumları ele almadan önce hacktivistlerin kökenleri ve yönelimlerinden kısaca bahsetmekte fayda vardır. Zira kökenleri ve yönelimleri, hacktivist oluşumlarının benimsedikleri felsefelerinin ve bu felsefe doğrultusunda gerçekleştirilen eylemlerinin büyük oranda belirleyicisi olarak görülmektedir.

Samuel'e (2004: 36) göre; hacktivizmin hangi formda ortaya çıkacağının iki temel belirleyicisi vardır. Bunlardan birincisi hacktivistlerin hangi kökenden geldiği, bir diğeri ise yönelimlerinin ne olduğudur. Hacktivistler, hacker-programcı ve sanatçı-aktivist olmak üzere iki farklı kökenden gelmektedir. Yönelimden kasıt ise suç teşkil eden eylemlere ne derece eğilimleri olduğudur. Hacktivistlerin suça karşı iki farklı yönelimi bulunmaktadır. Bunlardan birincisi yasal boşluklardan faydalanmak, bir diğeri ise doğrudan yasaya aykırı eylemlerde bulunmaktır. Dolayısıyla hacktivizmi daha iyi anlayabilmek için, bu köken ve yönelimler ayrıntılı olarak ele alınmalıdır.

1.4.1.1. Hacktivistlerin Kökenleri

Samuel'e (2004: 39) göre hacktivistler; hacker-programcı ve sanatçı-aktivist olmak üzere iki kökenden gelmektedir. Hacker-programcı köken, internetin sosyal ve politik kültürünü temsil ederken, sanatçı-aktivist köken ise postmodern solu temsil etmektedir ve bu iki köken hem farklı hacktivist kimlikleri hem de gerçekleştirilen hacktivist eylemlerinin biçimlerini değiştirmektedir. Farklı kökenlerden gelen hacktivistlerin birbirlerine bakış açıları da farklılaşmaktadır. Hacker kökenliler, aktivist kökenlileri genellikle teknik olarak yetersiz bulurken, aktivist kökenliler ise hacker kökenlilerin insanlardan çok bilgisayarları önemsediğini düşünmektedir.

1.4.1.1.1. Hacker-Programcı Köken

İnternet dünyasının; kendine has bir kültürü, dünya görüşü, politik gündemi ve kendine has davranış kalıpları vardır. Hacker-programcıları ağ üzerinde birbirlerine sıkıca bağlayan ise internetin bu farklı yapısıdır. Esasında internet kültürünü ortaya çıkaran da bir anlamda hacker kültürüdür. İnternet ortaya çıkmadan önce bilgisayar üzerine çalışmalar yapan bilim adamları, araştırma görevlileri ve hatta bilgisayar meraklıları bulabildikleri merkezi bilgisayar sistemleri üzerinde kümelenmekteydi. 1969 yılında ise bu merkezi sistemleri bir araya getirme fikriyle birlikte ARPANET projesi hayata geçirilerek, bu alana ilgi duyan insanların anında ve dünya çapında iletişim kurmaları sağlanmıştır. Oluşturulan ağdaki kullanıcıların en önemli amacı ise bilgisayarlara, diğer ağlara ve bilginin kendisine erişmekti. Bu erişim dürtüsü ise bir anlamda önceki bölümlerde ele alınan hacker etiğini de ortaya çıkarmıştır (Samuel, 2004: 39-41).

Hacker etiği olarak sıralanan maddeler, bilginin paylaşılması, geliştirilmesi ve insanların yararına kullanılmasının bir anlamda hackerların üstlendiği bir misyon olduğunu göstermektedir. Ancak günümüzde, bilginin güçle eşdeğer olması ve önemli bir ticari değer taşıması, hackerların arzu ettiğinin aksine bilginin paylaşılmasına değil, saklanmasına neden olmuştur. Bu durum bilgiyi özgürleştirmek isteyen hackerların aykırı duruşlarının temel sebebini oluşturmaktadır. Dolayısıyla çoğunlukla apolitik olarak görülen hackerların, gerçekte hiç de öyle olmadığı, hackerlığın temel felsefesi gereği politik bir duruş göstermeleri gerektiği açıkça görülmektedir.

Samuel (2004), hackerların neden apolitik değil politik olduklarını oldukça net çıkarımlarla özetlemektedir. Samuel'e (2004: 42) göre; hackerların en çok üzerine eğildiği konular; konuşma özgürlüğü, mahremiyet hakkı, entelektüel mülk özgürlükleri, herkese açık standartlar ve ücretsiz ve açık kaynak yazılımlardır. Daha açık bir ifadeyle hackerlar; konuşma özgürlüğüne müdahale olarak görülen çevrimiçi sansür gibi uygulamalara, otoritelerin çevrimiçi gözetimleri sebebiyle mahremiyet alanlarına müdahale etmesine, telif hakları iddiasıyla müzik, kitap, video vb. şeylerin paylaşılmaması veya bilginin özgürleştirilmemesine, teknoloji firmalarının ticari kaygılar sebebiyle İnternet'in karşılıklı işbirliğini garanti altına alan açık standartlarını sınırlandırmalarına ve son olarak teknolojiyi sürekli geliştirme

ihtiyaçlarına yönelik kısıtlamalara karşı, hackerlığın doğası gereği politik bir duruş sergilemektedirler.

1.4.1.1.2. Sanatçı-Aktivist Köken

Sanatçı-aktivist köken postmodern solun hacktivizm üzerindeki yansımasıdır. Postmodern sol kavramı ise; politik inanışların, teorik dünya görüşlerinin ve taktiksel inovasyonların bir kombinasyonu olarak nitelendirilmektedir. Dolayısıyla bu kökenden gelen hacktivistler, hacker-programcı kökenden gelenlerin aksine bilginin özgür olması vb. konulardan daha çok; küreselleşme, şirketlerin güçlenmesi, insan hakları ve çevresel sorumluluk gibi konulara eğilmektedirler (Samuel, 2004: 44-48). Bu bağlamda, bahsi geçen konularda tepki uyandıran herhangi bir kişi veya kuruluş bu kökenden gelen hacktivistlerin hedefinde yer alabilmektedir. Örneğin, Strano Network adlı grup, Fransa'nın nükleer ve sosyal konularla ilgili politikalarına tepkilerini göstermek amacıyla 21 Aralık 1995 tarihinde sanal oturma eylemlerinin uygulamadaki ilk örneklerinden birini gerçekleştirmiştir. Belirlenen saatte, dünyanın farklı yerlerinden katılımcılar tarayıcılarını hükümet sitelerine yönlendirerek internet trafiğine önemli ölçüde zarar vermiş ve bazı siteler bir süreliğine devre dışı bırakılmıştır (Denning, 2001: 264).

1998 yılında, Electronic Disturbance Theather adlı hacktivist oluşumun elektronik sivil itaatsizlik kavramını bir adım öteye taşıyarak, Zapatistalara olan desteklerini göstermek adına; başta Meksika başkanı Zedillo'nun web sitesi olmak üzere, Başkan Clinton'ın web sitesine ve Pentagon'un web sitelerine, School of Americas'a, Frankfurt ve Meksika Menkul Kıymetler Borsalarına yönelik gerçekleştirdikleri sanal oturma eylemleri de buna verilebilecek diğer bir örnektir. Bu hedeflerin seçilme nedeni ise; bu hedeflerin bir şekilde Zapatistlara karşı olduğu ve onların aleyhine çalıştığı düşüncesidir. Örneğin; Pentagon'un hedef olarak seçilmesinin nedeni, Birleşik devletler ordusunun, Zapatistalara yönelik insan hakları ihlalleri gerçekleştiren askerleri eğitmesidir. Frankfurt Menkul Kıymetler Borsası ise; soykırım ve etnik temizlikte kapitalizmin rolünü temsil ettiği için hedef olarak seçilmiştir (Denning, 2001: 264-265).

Benzer örneklerin sayısı oldukça fazla olmakla birlikte, burada değinilmek istenen nokta sanatçı-aktivist kökenden gelen hacktivistlerin odak noktalarının;

küreselleşme, insan hakları ihlalleri vb. hususlar olduğudur. Bu kökenden gelen hacktivistlerin sanatçı-aktivist olarak adlandırılmalarının temel sebebi ise; eylemlerinin estetik ve yaratıcılıkla bezenmesidir.

1.4.1.2. Hacktivistlerin Yönelimleri

Samuel'e (2004: 48-50) göre; hacktivizmin farklı türlerde ortaya çıkmasına neden olan ikinci değişken, hacktivistlerin suç işlemeye yönelik eğilimleridir – burada suç işlemekten kasıt bilgisayar ve internet suçu olarak görülen eylemlerin gerçekleştirilmesidir. Örneğin bazı hacktivistler; web site tahribatları, yönlendirmeleri, DoS saldırıları vb. suç kapsamında olan eylemleri gerçekleştirme eğilimindeyken, diğerleri ise; sanal oturma eylemleri gibi yasallığı muğlak olan eylemleri gerçekleştirme eğilimindedirler. Bu iki farklı yönelimi ortaya çıkaran dört temel özellik bulunmaktadır. Bu özellikler; yasal riske karşı gösterilen tolerans, şeffaflık, kolektif eylemin boyutu ve çokuluslu işbirliğinin yoğunluğu olarak sıralanmaktadır.

Tablo 3: Hacktivist Yönelimlerin Özellikleri

		Yönelim	
		Suçtan kaçınan	**Suça Yönelen**
Özellikler	**Yasal Risk**	Yasallığı muğlak	Açıkça yasaya aykırı
	Şeffaflık	Gerçek isimler, takip edilebilen rumuzlar	Takip edilemeyen rumuzlar, anonim
	Grubun Büyüklüğü	Orta ölçekli gruplar, kitlesel katılıma bağlılık	Bireysel, küçük gruplar
	Uluslararası İşbirliği	Çok uluslu (Birden fazla ulustan hacktivist ile birlikte çalışmak)	Ulusal (kendi ülkesi gibi) Çok uluslu (Sınırlar ötesi işbirliği) Uluslararası (uluslararası çatışmaları yansıtmak)

Kaynak: Samuel, 2004: 37

Hacktivistlerin yasal olmayan eylemleri gerçekleştirmeye yönelik isteklilikleri, bir başka ifadeyle yasal risk alma isteklilikleri farklılık göstermektedir. Suça yönelimli hacktivistler, DoS saldırıları gibi suç kapsamındaki eylemleri gönül rahatlığıyla gerçekleştirirken, yasalardan kaçınma yönelimli hacktivistler ise sanal

oturma eylemleri gibi en azından yasalar kapsamında suç olarak tanımlanmayan eylemleri tercih etmektedirler. Doğal olarak, suç teşkil eden eylemleri gerçekleştirenler arkalarında iz bırakmamak için kimliklerini genellikle gizli tutmakta, bir başka ifadeyle anonim olarak gerçekleştirmekte ve şeffaflıktan kaçınmaktadırlar. Buna karşın, eylemleri suç kapsamında yer almayanlar aynı kaygıyı taşımadığından kimliklerini gizli tutma gereği duymamakta, hatta kimliklerinin bilinmesini istemekte, dolayısıyla şeffaf olmaktan yanadırlar. Kolektif eylemin boyutu olarak tanımlanan üçüncü özellik ise; eylemin bireysel, küçük gruplar veya büyük gruplar halinde yapılmasını ifade etmektedir. Geleneksel kitlesel eylem biçimlerine kıyasla hacktivizmin bireysel olarak da ortaya çıkabilmesi, hacktivizmin çekici unsurlarından biri olarak görülmektedir. Son olarak ise; yapılan eylemlerin sınırları – daha açık bir ifadeyle ulusal veya uluslararası katılım olması- hacktivist yönelimleri belirleyen önemli bir özellik olarak ortaya çıkmaktadır. Bazı hacktivist eylemler sadece bir ülkedeki hacktivistlerin katılımıyla gerçekleştirilirken, bazıları ise küresel katılımlarla gerçekleştirilmektedir. Tablo 3'te, suça yönelim ve suçtan kaçınma yönelimi olarak da adlandırabileceğimiz iki farklı yönelimi açıklayan dört temel özelliğe ilişkin farklılıklar gösterilmektedir.

1.4.1.3. Samuel'in (2004) Tipolojisi

Samuel'e (2004) göre hacktivistler, kökenleri ve yönelimlerine göre farklı tiplerde hacktivist oluşumlar ortaya çıkarmaktadır. Hacker-programcı kökenden gelen ancak suç yönelimli olmayan hacktivistleri politik kodlayıcılar, bu kökenden gelen ancak suç yönelimli olanları ise politik kırıcılar olarak ele almaktadır. Edimsel hacktivistler ise sanatçı-aktivist kökenden gelen ancak suç yönelimli olmayan hacktivistleri temsil etmektedir. Tablo 4'te kökenleri ve yönelimlerine göre ortaya çıkan farklı tipler gösterilmektedir.

Tablo 4: Hacktivistlerin Kökenleri ve Yönelimlerine Göre Hacktivizm Tipleri

		Hacktivist Kökenler	
Hacktivist Yönelimler		Hacker-programcı dünyası	Sanatçı-aktivist dünyası
	Suçtan kaçınan	**Politik kodlayıcılar**	**Edimsel hacktivizm**
	Suça yönelen	**Politik kırıcılar**	

Kaynak: Samuel, 2004: 36

1.4.1.3.1. Politik Kırıcılar

Yasal olmadığı açıkça belli eylemleri gerçekleştiren hacker kökenli hacktivistleri kapsayan politik kırıcılık, gerek gerçekleştirilen eylemlerin sayısı, gerekse site tahribatı, site yönlendirmeleri, DoS saldırıları, bilgi hırsızlığı ve sabotaj gibi kullandıkları yöntemlerinin çeşitliliğiyle diğer iki tipten ayrılmaktadır. Eylemlerinin yasal olmaması sebebiyle anonim olarak gerçekleştirmekte ve bireysel veya küçük gruplar halinde çalışmaktadırlar. Tek başına bir web sitesini tahrip eden veya başka sitelere yönlendiren hacktivistlerin medyanın ilgisini önemli ölçüde çekebilmesi mümkündür. Yine de, politik kırıcıların az sayıda kişiden oluşan gruplar oluşturdukları da bilinmektedir. Ancak hack eylemlerini gerçekleştirenlerin anonim olması, eylemin grubun tüm üyeleri tarafından mı yoksa sadece bir veya iki üyesi tarafından mı yapıldığının anlaşılmasına imkan vermemektedir. Diğer iki hacktivizm tipinden farklı olarak ise, politik kırıcılık minimum düzeyde de olsa hacker topluluğu dışındakilerin bilemeyeceği bir kod bilgisi ve hackleme tekniklerine aşina olmayı gerektirmektedir (Samuel, 2004: 51-55).

Politik kırıcı oluşumlara verilebilecek en iyi örneklerden biri World's Fantabolous Defacers'tır. Kasım 2000'de ortaya çıkan bu grup, özellikle Hindistan ve İsrail karşıtı eylemlerde bulunmuştur. Sadece 20 Kasım 2000 ve 21 Kasım 2002 tarihleri arasındaki bilinen içerik bozma eylemlerinin sayısı 349'u bulmaktadır ki bu eylemlerden 26'sı birden fazla sitenin tahrip edilmesini içermektedir. Ancak internet arşivlerinde yer almayan saldırılar da hesaba katıldığında tahmini sayı 400'ü geçmektedir. Grubun gerçekleştirdiği eylemlerin büyük çoğunluğu, Filistin, Irak, Kashmir, Çeçenistan vb. bölgelerdeki Müslümanlara yönelik insan hakları ihlalleri konusunda küresel farkındalık yaratmak amacıyla yapılmıştır (Samuel, 2004: 56-57).

Yukarıdaki örnekten de anlaşılacağı üzere, bu tip hacktivizm çoğunlukla uluslararası problemlerden doğmaktadır. Bu örneğin bir benzeri Doğu Timor'un bağımsızlık sürecinde yaşanmıştır. Eylül 1998'de, Portekizli hackerlar 40 Endonezya sunucusundaki siteleri değiştirerek "Doğu Timor'a Özgürlük" mesajını yerleştirmiş ve buna ek olarak burada gerçekleştirilen insan hakları ihlallerini gösteren linkler eklemişlerdir. Ağustos 1999'da, Doğu Timor bağımsızlık hareketini destekleyen Nobel barış ödüllü Jose Ramos Horta, Jakarta'nın Doğu Timor'un özgürlüğüne yönelik oylamayı sabote etmesi halinde küresel bir hacker ağının Endonezya'yı

durma noktasına getirmeye yönelik planları olduğu yönünde uyarılarda bulunmuştur (Denning, 2001: 272). Hacktivistlerin Doğu Timor bağımsızlık hareketi sırasında yaptıklarının ne derece etkili olduğu tartışılabilir olsa da, Endonezya 1999 yılında Doğu Timor üzerinde hak iddia etmekten vazgeçmiş ve 1999 yılında yapılan referandumun ardından Doğu Timor 2002 yılında bağımsızlığını kazanmıştır.

1.4.1.3.2. Edimsel Hacktivizm

Edimsel hacktivizm; politik amaçlar doğrultusunda yasallığı muğlak eylemleri gerçekleştiren sanatçı-aktivist kökenli hacktivistleri temsil etmektedir ve sol politik kültürden geldiği için; küreselleşme, şirketlerin güçlenmesi, özgürlük mücadeleleri gibi konularla ilgilenmektedir. Bu bağlamda bu hacktivistlerin gerçekleştirdikleri eylemlerin, aktivistlerin geleneksel sokak eylemleriyle eşzamanlı olması şaşırtıcı değildir. İlgilendikleri sorunların yelpazesi oldukça geniş olabilse de; daha çok küreselleşme ve insan hakları gibi çevrimdışı konulara odaklanmaları, sanal oturma eylemleri gibi örgütlü hareketleri ana eylem biçimleri olarak ortaya çıkarmaktadır. Her ne kadar bu sanal oturma eylemleri çekirdek hacktivist gruplar tarafından organize edilse de, etkisinin hissedilebilmesi için yüksek düzeyde katılım gerektirmesi bakımından çoğunlukla küresel çapta katılımcıların desteğini almaktadır. Bu eylemlerde hacktivist grupların üstlendiği esas rol ise; eylemlerin planlanması, organize edilmesi ve katılımcıların işlerini kolaylaştıracak yazılımlar üretilmesidir. Örneğin; pek çok hacktivist grup, planlanan eylemlerin gerçekleştirilebilmesi için sanal oturma eylemleri ve web site parodileri için otomatikleştirilmiş yazılımlar geliştirmektedir (Samuel, 2004: 71-72).

Kullandıkları taktikleri oluşabilecek yasal risklerden kaçınmak için dikkatlice planlamaktadırlar. Nitekim sanal oturma eylemleri; birden fazla kullanıcının aktif katılımını ve gerçekten hedefteki sitenin web sitesine erişmeyi gerektirmesi bakımından DoS saldırılarına kıyasla daha yasal olduğu açıkça görülmektedir (Samuel, 2004: 73). Sonuçta, sanal oturma eylemlerini gerçekleştiren katılımcıların otomatikleştirilmiş yazılımlar yardımıyla da olsa; hedefteki web sitesine kendi bilgisayarlarından erişim sağlamaları ve site üzerindeki trafiği bu sayede arttırmaları yasalara pek de aykırı görünmemektedir. Bunun aksine, DoS saldırıları ise tek bir

hacker tarafından birden fazla bilgisayara erişim sağlayarak gerçekleştirilebilmesi bakımından kitlesel bir protestoyu yansıtmamaktadır.

Edimsel hacktivistlerin temel kaygısı kamuoyunda farkındalık yaratmak ve şirketler ve medya üzerinde kamuoyu baskısı oluşturmaktır (Samuel, 2004: 73). Daha açık bir ifadeyle, şirketlerin ve medyanın kamuoyunun yönlendirilmesi hususundaki baskın rolleri hacktivistlerin tepkilerini çekmekte ve onlara göre gerçeklerin kamuoyu tarafından bilinmesi için bu eylemler gerçekleştirilmektedir. Ancak bu hacktivistlerin hedefinde sadece ticari kuruluşlar değil; Uluslararası Para Fonu (IMF) ve Dünya Ticaret Örgütü gibi küresel oluşumlarla birlikte yerel hükümetler de yer alabilmektedir. Sol görüş kültüründen gelen bu hacktivislerin; devletler, işletmeler ve uluslararası kuruluşları birbirlerine bağlı bir zincir ve kapitalizm ve küreselleşme gibi olguların en sıkı destekçileri olarak görmeleri ve bu sebeple hedef seçmeleri pek de şaşırtıcı değildir.

Bu gruba mensup hacktivist oluşumların ilk örneklerinden biri daha önce de sözü edilen Electronic Disturbance Theater'dır (EDT). Bu grubun temel felsefesine göre, devlet dışı aktörlerin de mevcut ve gelecek çatışma alanlarında söz hakkı vardır ve sanal alem diğer aktörlerin bu sahnede olması için bir araçtır. Nitekim Zapatista özgürlük hareketine verdikleri destek bu felsefelerini açıkça göstermektedir. Benzer şekilde, Electrohippies Collective adlı diğer bir hacktivist gruba göre ise; yaptıkları sanal oturma eylemleri siyasi konulardaki geniş tartışma alanlarında söz hakkı olması gereken, ancak sesini yeterince duyuramayan gruplar adına yapılmalı ve oturma eylemlerini meşru kılmak için yapılan etkinlik bu tartışma alanlarına odaklanmalıdır (Denning, 2001: 266-268).

1.4.1.3.3. Politik Kodlayıcılar

Hacker kökenli ve suçtan kaçınma yönelimi olan politik kodlayıcıların odaklandıkları konular, özellikle çevrimiçi haklar gibi bireysel haklardır. Bunun sebebi ise; bu gruptaki hacktivistlerin hacker topluluğunun benimsediği bilginin özgür ve ticarilikten uzak olması, mahremiyet hakları gibi değerlerini savunması ve sansür ve çevrimiçi gözetim gibi uygulamalara karşı çıkmalarıdır. Özellikle anti demokratik ülkelerde görülen çevrimiçi sansürün önüne geçebilmek adına oldukça etkili yazılımlar geliştirmişlerdir. Bu hacktivist sınıfın ilk eylemleri Legions of the

Underground adlı hacktivist oluşumun Çin'deki çevrimiçi sansürü protesto etmek için gerçekleştirdikleri hack eylemleriyle başlamıştır. Buna ek olarak, yayınladıkları bir bildiriyle bilgiye erişim özgürlüğünün Çin hükümeti tarafından engellendiğini ve bu sebeple diğer hacktivistlerin de davalarına destek vermelerini istemişlerdir. Bu çağrı daha sonra çeşitli hacktivist grupların desteğini alarak sansürü delmek adına çeşitli anti sansür uygulamaları ve projeleri geliştirilmesini sağlamıştır. Bu projelerden ilki ve belki de en önemlisi ise Cult of the Dead Cow adlı oluşumun ortaya attığı Hacktivismo projesidir. Bu projenin temel amacı Çin vb. ülkelerdeki çevrimiçi sansürü kırabilmek ve bu ülkelerdeki internet kullanıcılarının bilgiye erişimini sınırsız kılabilmek için çeşitli yazılımlar geliştirmekti (Samuel, 2004: 88-97).

Özellikle son yılllarda, çevrimiçi gözetim uygulamaları etkisini arttırmış ve çeşitli web sitelerine erişim imkanları pek çok hükümet tarafından kısıtlanmıştır. Ancak politik kodlayıcıların açtığı bu yolda, özellikle bu gözetime tepkili olanlar her zaman yasakları delmenin bir yolunu bulmuşlardır. Örneğin web tarayıcılarına Zenmate vb. herhangi bir eklenti ekleyerek kolaylıkla çevrimiçi gözetimden kaçınılabilmektedir.

Politik kodlayıcılar da edimsel hacktivistler gibi açıklık ve şeffaflıktan yanadırlar. Bu sebeple kimliklerini gizli tutma gereği duymamakta, izi sürülebilen rumuzlar kullanmaktadırlar. Edimsel hacktivistlerle benzeşen diğer yönleri ise kolektif eylemden yana olmaları ve suç kapsamına giren eylemlerden kaçınmalarıdır. Özellikle çevrimiçi sorunlarla ilgilenmeleriyle de politik kırıcılarla benzeşmektedir-ancak politik kırıcıların ilgilendiği sorunların kapsamı insan hakları gibi sorunları da kapsayacak şekilde genişlemiştir. Bu üç hacktivizm tipini birbirlerinden ayıran en önemli nokta ise yönelim ve köken bakımından farklı olmaları sebebiyle kullandıkları yöntemlerdir. Örneğin; politik kırıcılar web site tahribatları, bilgi hırsızlığı, DoS saldırıları gibi yöntemleri benimserken, edimsel hacktivistler sanal oturma eylemleri ve web parodileri gibi yöntemleri, politik kodlayıcılar ise yasal yazılımlar geliştirme yöntemini benimsemektedirler (Samuel, 2004: 97-101).

1.4.2. Jordan ve Taylor'ın (2004) Hacktivizme Tipolojik Yaklaşımı

Jordan ve Taylor'a (2004: 67-69) göre hacktivizm; kitlesel eylem hacktivizmi ve dijital doğrucululuk hacktivizmi olmak üzere iki biçimde ortaya çıkmaktadır. Bu farklılığı doğuran temel sebep ise; hacktivistlerin odak noktalarının farklı olmasıdır. Kitlesel eylem hacktivizmi daha çok küreselleşme karşıtlığı gibi çevrimdışı hareketlerin sanal alemdeki yansıması olarak görülmekteyken, dijital doğruculuk hacktivizmi ise; tamamen çevrimiçi konulara odaklanmakta ve hack eylemlerinin tarihi ve teknik hususlarıyla, bir başka ifadeyle hacker etiği olarak daha önce de ele alınan bilginin özgür olması ve herkes tarafından erişilir olması gibi temel problemlerle ilgilenmektedir. Ancak her iki trendin de ortak noktası doğrudan eylem biçimlerini benimsemeleridir. Doğrudan eylem kavramı ile anlatılmak istenen, ani bir politika değişikliği sağlama girişimidir ve boykotlar, kuşatmalar, grevler ve sivil itaatsizlik gibi taktikleri bünyesinde barındırmaktadır. Söz konusu hacktivizm olduğunda doğrudan eylem kavramını sanal olarak nitelendirmek de bir gereklilik halini almaktadır. Bu bağlamda, çevrimiçi doğrudan eylem kavramı karşımıza çıkmakta ve geleneksel protesto biçimlerinin sanal alem için yeniden yaratılmasını ifade etmektedir.

Doğrudan eylemin temel amacı ani bir politika değişikliği sağlamaktır. Yasalardan kaçınmak veya onları önemsememek mümkün olsa da, yapılan eylemler herhangi bir yasa değişikliği sonucunu doğurmuyorsa, bu durum hedeflenen sonuca ulaşılamadığı ve eylemin başarısız olduğu anlamına gelmektedir. Hacktivizm söz konusu olduğunda da, doğrudan eylem kavramının temel prensipleri geçerlidir. Örneğin bir sokak protestosu düzenleyerek gerçekleştirilmek istenen bir buluşma engellenmek istenilebilir. Bunun sanal versiyonu ise; çevrimiçi mesajların ilgili kişilere ulaşmaması için sanal bir kuşatma yaparak, düzenlenmek istenen toplantıların engellenmesini sağlamaktır (Jordan ve Taylor, 2004: 68-69).

Özetle doğrudan eylem kavramının önerdiği üzere, hacktivizm faaliyetlerinin de temel amacı bir politika değişikliği sağlamaktır. Gerek kitlesel eylem hacktivizmi, gerekse dijital doğruculuk hacktivizmi bu ortak prensipleri benimsemeleri bakımından benzeşmektedirler. Aşağıda Jordan ve Taylor'un (2004) hacktivizmin iki farklı trendi olarak ele aldığı bu hacktivizm tipleri ayrıntılı olarak ele alınmaktadır.

1.4.2.1. Kitlesel Eylem Hacktivizmi

Kitlesel eylem hacktivizmi; "siyaset ve verimsiz teknolojinin bir kombinasyonudur. Birbirlerini henüz tanımayan sanal bedenlerin kitlesel yığınların yararına olacak şekilde, çevrimiçi hayatın fiziksel yetersizliğine karşı durma girişimidir. Kitlesel eylem hacktivizmi, geleneksel kitlesel protestoların internete yansıyan halidir" (Jordan ve Taylor, 2004: 69).

Jordan ve Taylor'a göre (2004, 69) Critical Arts Ensemble adlı aktivist oluşumun "elektronik sivil itaatsizlik üzerine" ilk olarak 1994 yılında yayınladıkları kitap ve bu kitapta ortaya atılan fikirler, hacktivizm açısından önemli bir dönüm noktası olarak görülmektedir. Nitekim CAE sözü geçen yayında geleneksel protesto biçimlerini sıklıkla eleştirmiş ve güç odaklarının özellikle küreselleşme ve internet çağında durağanlıktan çıkarak dinamik bir yapıya büründüğünü, buna karşın aktivistlerin geleneksel protesto yöntemlerini sürdürdüklerini öne sürmüştür. Dolayısıyla sadece, aktivistlerin eylem biçimlerinin sanal ortam için yeniden yaratılması yoluyla, istenen politika değişikliklerinin gerçekleştirilebileceğini savunmuşlardır.

CAE'ye göre (1996: 7-32); eylemlerin hedefinde hangi kuruluş olursa olsun, değer taşıyan varlıkların (para, bilgi vb.) artık sanal ortamda var olmaları ve sermayenin herhangi bir yere kolaylıkla taşınabilmesi gibi sebeplerle, geleneksel protesto biçimlerinin etkisi sınırlı kalmaktadır. Dolayısıyla yapılan eylemlerin tesirli olabilmelerinin tek yolu sanal ortamdaki bilgi akışını engelleyebilmektir. Bunu sağlayabilmek için ise; hackerların ve aktivistlerin ortak bir platformda buluşmaları gerekmektedir. Ancak çeşitli güçlükler bu birleşmeyi zorlaştırmaktadır. Öncelikle hackerların, gerek yeterli donanıma sahip olmak için harcadıkları zaman, gerekse harcanan zaman sebebiyle kendileri dışındaki insanlarla yeterli iletişim kuramamaları, onların siyasi konular hakkındaki bilgiye erişimini sınırlandırmaktadır. Aktivistler açısından bakıldığında ise temel problem, geleneksel kalıplarının dışına kolay kolay çıkmamaları ve düşünce ve eylem biçimlerine sıkı sıkıya bağlı olmalarıdır. Aktivistler, doğru hedefin seçimi ve ne yapılacağı konusunda bilgi sahibi olsalar da; bunları gerçekleştirmek için hackerların sahip olduğu etkili araçlardan mahrumlardır. Dolayısıyla bu kesimlerin birleşimi vasıtasıyla, etkili eylemler gerçekleştirebilmek mümkün olabilecektir. CAE'nin

elektronik sivil itaatsizlik üzerine yaptığı bu çağrı, ilerleyen yıllarda etkisini daha fazla hissettirmiş ve hacktivizmin doğuşunda önemli bir rol üstlenmiştir. Nitekim CAE'nin hackerların ve aktivistlerin bir araya gelmesi gerektiğine yönelik önerisi tam olarak hacktivizmi özetlemektedir. Bu oluşumun bir parçası olan Ricardo Dominguez daha sonra Electronic Disturbance Theater adlı hacktivist grubun kurucuları arasında yer almış ve CAE'nin elektronik sivil itaatsizliğe yönelik görüşlerini, pratikte gerçekleştirme fırsatı bulmuştur. EDT'nin Zapatista isyanı sırasında özellikle Meksika ve ABD hükümetlerinin web sitelerine yönelik gerçekleştirdikleri sanal oturma eylemleri, kitlesel eylem hacktivizmine verilebilecek en iyi örneklerden biridir (Jordan ve Taylor, 2004: 72).

Kitlesel eylem hacktivizminde küreselleşme karşıtı hareketlerin önemli bir yeri vardır ve sıklıkla sokak protestolarıyla eş zamanlı eylemler yapılmaktadır. Bu eylemlerden en önemlilerinden biri, küreselleşme karşıtlarının önemli bir hedef olarak gördüğü Dünya Ticaret Örgütü'ne karşı 1999 yılında gerçekleştirilmiştir. Dünya Ticaret Örgütü'nün Seattle'da gerçekleştirdiği toplantıları engellemek için aktivistler çeşitli sokak protestoları düzenlemiştir. Bu eylemlerle eş zamanlı olarak ise Electrohippies adlı hacktivist oluşum, bilgi akışını engelleyebilmek için DTÖ'nün konferans ağlarına yönelik DDoS saldırıları düzenlemiştir. Bu eylemler sırasında, 5 gün içerisinde 450000 kişi (veya bilgisayar) bu engelleme girişimlerine katılmıştır. Electrohippies, geliştirdiği bir yazılım vasıtasıyla DTÖ'ye yönelik eylemlere katılmak isteyen kullanıcıların hedefteki DTÖ bilgisayarlarına sürekli olarak ping atmasını sağlamış ve bu sayede DTÖ ağları yavaşlamış veya işlem göremez hale gelmiştir. Bu eylemlerin kitlesel eylem hacktivizmi olarak nitelendirilmesinin en önemli sebebi ise, sadece bir veya birkaç kullanıcının farklı bilgisayarlara erişim sağlayarak gerçekleştirdiği saldırıların aksine, kullanıcıların aktif olarak eyleme katılma gerekliliğidir. Daha açık bir ifadeyle bu saldırılar sırasında on binlerce insan aktif olarak bu hedeflere yönelik kişisel bilgisayarlarından, Electrohippies'in geliştirdiği yazılım vasıtasıyla saldırıları gerçekleştirerek kitlesel bir eyleme imza atmışlardır (Jordan ve Taylor, 2004: 74-79).

Şirketlerin zaman zaman gerçekleştirdikleri agresif eylemler, onların sıklıkla kitlesel eylem hacktivistlerinin tepkisini çekmesine neden olmaktadır. 1999 yılında gerçekleştirilen etoy savaşları veya etoy kampanyası olarak bilinen eylemler bunun

en tipik örneğidir. İnternet üzerinde oyuncak satan ve 29 Kasım itibariyle borsadaki işlem fiyatı 67 USD olan www.etoys.com, www.etoy.com adlı bir sitenin var olduğunu öğrendiğinde, bunun firmanın ticari kazançlarını olumsuz yönde etkileyeceğini düşünerek öncelikle bu siteyi satın almaya çalışmış, ancak siteyi satın alamayınca mahkeme kararıyla kapatmaya çalışmıştır. Etoys'un bu agresifliği, hem çevrimiçi hem de çevrimdışı pek çok grubun tepkisini çekmiş ve çeşitli eylemlerin yapılmasına sebep olmuştur. Çevrimdışı topluluklar etoy.com'un yasal yollardan hakkını aramakla ilgilenirken, çevrimiçi topluluklar ise çeşitli inisiyatifler kurarak 2 hafta boyunca Etoys'un ağlarına saldırmıştır. Bunlara ek olarak, Etoys ile ilgili farkındalık yaratmak adına ayna siteler kurulmuş ve şirket personeline sürekli olarak patronlarının eylemleriyle ilgili e postalar gönderilmiştir. Bu saldırıların bitişi ve savaşın kazanılmasının ardından şirketin hisse senetleri yaklaşık %70 değer kaybederek 19 USD'ye gerilemiştir. Bu değer kaybında Toys "R" Us firmasının Etoys'a rakip olarak ortaya çıkması önemli bir faktör olarak görülse de havktivist eylemlerin de bunda payının olduğu gözle görülür bir gerçektir. Nitekim yasal mücadeleler, internet saldırıları ve etkili medya kampanyaları sayesinde Etoys www.etoy.com'u kapatma girişimlerinden vazgeçmiştir (Jordan ve Taylor, 2004: 83-84).

Sonuç olarak; EDT ve Electrohippies adlı hacktivist grupların eylemleri ve etoy savaşları gibi vakalar, hükümetler, uluslararası kuruluşlar ve ticari işletmeler gibi pek çok farklı kuruluşun, gerek ideolojik sebeplerle, gerekse bu kuruluşların eylemleri sebebiyle hedef olarak seçilebildiklerini göstermektedir. Ancak bu eylemlerin kitlesel eylem hacktivizmi olarak değerlendirilmesinin temel sebebi, bireylerin kendi rızalarıyla çeşitli hack tekniklerinden faydalanarak, güç odaklarına karşı internet üzerinde sergiledikleri kitlesel protestoları nitelendirmesidir.

1.4.2.2. Dijital Doğruculuk Hacktivizmi

Electronic Disturbance Theater vb. hacktivist oluşumlar sıklıkla otomatikleştirilmiş yazılımlar vasıtasıyla DDoS saldırıları düzenleyerek kullanıcıların internet erişimlerini engellemektedirler. Yine de bu tür eylemler bazı hacktivist gruplar tarafından hoş karşılanmamaktadır. Özellikle hacker kökenli hacktivistler, hack kültürünün gereği olarak internete erişimin en temel bireysel

haklardan biri olduğunu ve hiçbir şekilde engellenmemesi gerektiğini savunmaktadırlar. Nitekim Turkle (2005: 205) hack kültürünü; eşyalarla ilişkilerde karmaşıklığa ve riske değer veren, ancak insan ilişkilerinde basitlik ve güvenlik arayan bir uzmanlık ve bireycilik kültürü olarak özetlemiştir. Ancak daha önce de sözü edildiği gibi çoğu kesim bu görüşü tam olarak desteklememekte, hacker kökenlilerin insanlardan çok bilgisayarları ve ağları önemsediğini savunmaktadırlar. Jordan ve Taylor'un (2004) dijital doğruculuk hacktivizmi olarak tanımladıkları erişim hakkı vb. çevrimiçi hakların engellenmemesi gerektiğini savunan bu anlayış, aynı zamanda Samuel'in (2004) politik kodlayıcılar olarak betimlediği hacktivizm tipiyle benzeşmektedir. Jordan ve Taylor'a (2004: 69) göre dijital doğruculuk hacktivizmi; "hack eylemlerinin sanal alemin alt yapısındaki politik uygulamalarıdır. Politik bir mesajı yaymak için, sanal hayattaki fiziksel yetersizliği kullanma girişimidir".

Dijital doğruculuk hacktivizmi de en temel bireysel hakları korumaya yönelik hareket etmektedir. Ancak burada sözü geçen temel hak bilgiye erişim hakkıdır. Bu trendi destekleyen hacktivistlere göre, bilgi özgür ve serbest olmalı ve erişim hakları hiçbir şekilde kısıtlanmamalıdır. Dolayısıyla erişim haklarını kısıtlayan her türlü oluşumla mücadele etmektedirler (Jordan ve Taylor, 2004: 96-97). Örneğin Çin, Singapur vb. ülkelerde bireylerin sadece belirli sitelere girmelerine izin veren, diğer sitelere ise erişimlerini engelleyen güvenlik duvarları bulunmaktadır. Dijital doğruculuk hacktivizmini benimseyenlerin en temel misyonu ise, bu bariyerleri yıkarak insanlara bilgiye ulaşma yollarını göstermektir. Cult of the Dead Cow gibi hacktivist oluşumlar, Hacktivismo vb. projeleri vasıtasıyla bu bariyerlerin yıkılmasında önemli roller oynamışlardır.

Bilginin serbest olması dijital doğruculuk hacktivizminin merkezinde yer almakta ve insanların bilgiye erişebilmeleri için internet kanallarını herkes için ulaşılabilir tutmaya çabalamaktadırlar. Bu bir anlamda kitlesel eylem hacktivistlerinin sanal ortamda gerçekleştirdikleri eylemler için de önemli bir fayda sağlamaktadır (Jordan ve Taylor, 2004: 114-115). Ancak dijital doğruculuk hacktivizminin, kitlesel eylem hacktivizmiyle birleştiği tek nokta bu değildir. Dijital doğrucu hacktivistler de bir anlamda politik olmak zorunda kalmışlardır. Bunun temel sebebi ise bilginin ticari olmaması gerektiğine inanmalarıdır. Günümüzde ise

bilgi taşıdığı ticari değer sebebiyle sıklıkla saklanmaktadır. Dolayısıyla dijital doğrucu hacktivistler bilgiye erişimi kısıtlayan her türlü kamu ve özel kuruluşa karşı mücadele etmektedir. Her ne kadar küreselleşme karşıtlığı olarak nitelendirilemese de, dijital doğruculuk hacktivizmi de tıpkı kitlesel eylem hacktivizmi gibi küresel güç odaklarıyla mücadele etmektedir. Bir başka ifadeyle, her ne kadar temel felsefeleri farklı olsa da, her iki trendin hedeflerindeki kuruluşlar sıklıkla kesişmektedir.

İKİNCİ BÖLÜM
KURUMSAL İTİBAR KAVRAMI, TANIMI VE ANLAMI, DİĞER KAVRAMLARLA İLİŞKİSİ, KURUMSAL İTİBAR KAVRAMINA YAKLAŞIMLAR VE KURUMSAL İTİBARIN ÖLÇÜMÜ

2.1. KURUMSAL İTİBAR KAVRAMI, TANIMI VE ANLAMI

20. yüzyılın son yıllarında küresel ekonomi ve gelişen ve değişen teknolojinin etkisiyle şirketlerin piyasa ve defter değerleri arasındaki fark giderek açılmaya ve piyasa değerlerinde bir yükseliş oluşmaya başlamıştı. Ancak 2001 yılından itibaren mevcut eğilim bir anda tersine dönmüş, istikrarlı olarak görülen firmalar kısa süre içinde piyasa değerlerinin önemli bir kısmını yitirmiş ve piyasalara kötümserlik hakim olmaya başlamıştır. Bu süreç neticesinde, firmaların piyasa değerleri ve defter değerleri arasındaki açıklığın tam olarak neden kaynaklandığını sorusu giderek önem kazanmıştır. Kimilerine göre ise, kurumsal itibar bu sorunun cevabı olarak ortaya çıkmıştır (Cravens ve diğerleri, 2003: 201).

İnsanlara en çok saygı duydukları şirketin hangisi olduğu sorulduğunda hepsi bir isim ve bir fikir belirtecektir. Kimileri bu ismi firmayla yaşadıkları doğrudan deneyimlere göre seçerken, bazıları da firmaya yaptıkları yatırımlardan elde ettikleri getiriye göre değerlendirecektir. Bu fikirlerin toplamı genel halkın fikirlerini temsil edebilecek düzeye geldiğinde, kurumsal itibarın o anlık görüntüsü elde edilmiş olacaktır (Fombrun ve Gardberg, 1999: 13).

Kurumsal itibar, "bir firmanın geçmişinden yola çıkılarak bu firmaya atfedilen özellikler dizisidir" (Weigelt ve Camerer, 1988: 443) ve bu özelliklere dair değer yargılarını ifade etmektedir (Gray ve Balmer, 1998: 697).

Kurumsal itibar; bir firmanın geçmiş eylemlerinin (Nguyen ve Leblanc, 2001: 228) ve bir kitle tarafından o firma hakkında zamanla elde edilen tam olmayan bilgilerin değerlendirilmesinin bir sonucudur (Caruana, 1997: 114).

Barnett ve arkadaşları (2006: 34) kurumsal itibarı; "gözlemcilerin bir firmaya atfettikleri finansal, sosyal ve çevresel etkilerin zaman içindeki birikimine göre yaptıkları değerlendirmelere dayanan yargılarının toplamı" olarak tanımlamaktadır.

Fombrun ve Rindova'ya (1996) göre ise, kurumsal itibar; bir firmanın tüm paydaşlarına değerli çıktılar verebilme kabiliyetini gösteren sonuçların ve firmanın

geçmiş eylemlerinin, kollektif bir yansımasıdır. Dolayısıyla, hem rekabet çevresi hem de kurumsal çevrede iç ve dış paydaşların gözünden bir firmanın göreceli yerini göstermektedir (Gardberg ve Fombrun, 2002: 304-305).

Kurumsal itibar tanımlanırken paydaşlardan ya da bir izleyici kitle grubundan ayrı olarak değerlendirilebilmesi mümkün görünmemektedir. Her bir paydaş grubu kendine has benzer geçmişe ve değer sistemlerine sahip olabilmekte ve bu sebeple algıları diğer paydaş gruplarının algılarından farklılaşmaktadır. Daha açık bir ifadeyle; firmalar birden fazla kitleye hitap ettikleri gibi, bu kitlelerin her biri farklı özelliklere dikkat etmekte ve bu özelliklerin önem derecesi de değişmektedir (Gray ve Balmer, 1998: 698-699; Walsh ve diğerleri, 2009b: 189). Bu durumda, bir dizi ya da birden fazla itibar algısından bahsedebilmek mümkündür. Örneğin, yöneticiler ve brokerlar finansal performansa dikkat ederken, tüketiciler ise, ürünün kalitesinin daha önemli olduğunu düşünebilmektedir. Dolayısıyla, tüketiciler firmanın itibarını değerlendirirken finansal performansını hiç umursamayabilmekte veya bu özelliğe düşük düzeyde önem verebilmektedir (Caruana, 1997: 110). O halde, firmaların itibarından söz ederken; ürün kalitesi itibarı, fiyat itibarı, yenilik itibarı, yönetim kalitesi itibarı ve "bir firmanın medyadaki genel değerlendirmesi" (Deephouse, 2000: 1091) olarak tanımlanan medya itibarı gibi birden fazla itibarı olabileceğini söylemek mümkündür (Nguyen ve Leblanc, 2001: 228).

Fombrun ve Shanley'e (1990: 252) göre, kamuoyundaki itibar algısı; finansal ve pazara dair bilgiler, medya raporları ve diğer ekonomik olmayan ipuçlarının karışımına göre oluşmaktadır. Firmaların risk-getiri profilleri, kaynak dağıtımları, sosyal sorumlulukları, kurumsal sahiplikleri, medyadaki yansımaları ve kurumsal çeşitliliğe yönelik duruşları firmaların geleceğine dair ipuçları vermekte ve itibarı oluşturmaktadır.

Shapiro (1982: 21) ise, zaman içinde herhangi bir noktada her bir müşterinin ürün kalitesine dair bazı beklentileri olduğunu belirtmekte ve bu beklentilerin itibarı oluşturduğunu öne sürmektedir.

Fombrun ve Rindova'ya (1996) göre; itibar firmaların güvenilirlikleriyle ilgili öznel ve kolektif değerlendirmelerden oluşmaktadır (Fombrun ve Van Riel, 1997: 10). Buna göre firmaların itibarları;

- Bir örgütsel alanda firmaların yeni (emergent) durumlarını belirginleştiren bir endüstriyel sistemin türev özellikleridir.
- Bir firmanın içsel kimliğinin dışsal yansımasıdır.
- Firmaların önceki kaynak dağıtımları ve geçmişlerinden gelişmektedir ve hem firmaların hem de rakiplerinin eylemlerini sınırlayan dolaşım engelleri meydana getirmektedir.
- Firmaları çeşitli kriterleri tatmin edebilme kabiliyeti ve potansiyeline göre değerlendiren çeşitli değerlendiricilerin firmanın geçmiş performansına yönelik değerlendirmelerini özetlemektedir.
- Paydaşların bir firmayla ilgili birden fazla ancak birbirleriyle ilişkili imaj algılarından türemekte ve çalışanlara, tüketicilere, yatırımcılara ve yerel halka firmanın genel çekiciliği hakkında bilgi sağlamaktadır.
- Firmaların etkililiğini gösteren iki ana boyutu olan firmanın ekonomik performansına ve firmanın sosyal sorumluluklarını yerine getirebilme başarısına yönelik değerlendirmeleri kapsamaktadır.

Yukarıdaki kavramsal itibar tanımları incelendiğinde, aralarında benzerliklerin yanında farklılıklar da içerdiği görülmektedir. İlgili alan yazında itibar üzerine pek çok çalışmada, itibar kavramının ne olduğu ve neleri içerdiği üzerine bir uzlaşı olduğu söylenemez (Castro ve diğerleri, 2006: 362). Örneğin Wartick (2002: 374-381), alan yazında en çok kabul gören tanım olan Fombrun'ın (1996) itibar tanımını birkaç açıdan eleştirmektedir. Wartick (2002), itibarın sadece paydaşların algılarından oluşmadığını ve firmaların geçmişine dair bilgilerin bazı bireyler tarafından işlenmesiyle firma hakkında sonuçlara ulaşmasının mümkün olduğuna değinmektedir. Dolayısıyla algıların tanımdaki merkezi rolünü eleştirmektedir. İkinci olarak ise, paydaşların itibar algılarının toplamı olarak ele alınmasının yanlış olduğunu iddia etmekte ve bu açıdan bakıldığında kavramın imaj ve kimlik kavramlarıyla karıştığını öne sürmektedir. Wartick'in (2002) eleştirdiği üçüncü nokta ise itibarın rakiplere göre tanımlanması durumudur. Wartick (2002) bu kıyaslamanın hangi standartlara (firmanın geçmiş performansı, rakipleriyle kıyaslanması, endüstri ortalaması vb.) göre yapıldığının önemli olduğunu belirtmektedir.

Bu bölümde, kurumsal itibar kavramına kısa bir giriş yapılmış olup, ilerleyen bölümlerde kurumsal itibar kavramına ilişkin karmaşa giderilmeye çalışılacaktır.

Bunun için öncelikle kurumsal itibar ekollerinin detaylı olarak ele alınması ve sonrasında ise kurumsal itibar ve bu kavramla ilişkili olarak görülen kavramların etraflıca tartışılması gerekmektedir.

2.2. KURUMSAL İTİBAR, KURUMSAL KİMLİK VE KURUMSAL İMAJ KAVRAMLARI ARASINDAKİ İLİŞKİ

Kimlik, imaj, prestij, iyi niyet, saygı ve duruş kavramları sıklıkla kurumsal itibarla eşanlamlı veya yakın ilişkili olarak ele alınmıştır. Bu terimlerden her biri; (a) ya itibarın dengi, (b) ya itibarın önemli bir parçası, (c) ya da itibarı da içine alan daha geniş bir yapı olarak ele alınmıştır (Wartick, 2002: 373).

Kurumsal itibara ortak bir tanım getirmenin zorluğu; imaj, kimlik ve itibar kavramları arasındaki karmaşıklıktan kaynaklanmaktadır (Caruana, 1997: 110; Barnett ve diğerleri, 2006: 28). Wartick'e (2002: 374) göre ise, farklı disiplinlerin itibar kavramına yönelik bakış açıları ve zaman zaman itibarı yukarıda sözü edilen kavramlarla eşanlamlı veya ilişkili görmeleri, itibar kavramını tanımlamayı zorlaştırmaktan çok, bu disiplinlerde ele alınan diğer kavramlardan farkını ortaya koymayı zorlaştırmaktadır.

Gray ve Balmer'a (1998: 695-696) göre, kurum kimliği, kurumun gerçekliğidir ve kurumun ayırt edici özelliklerini temsil ederek kurumun ne olduğu sorusuna yanıt vermektedir. Kurum kimliğinin temel bileşenleri ise; strateji, temel felsefe, kültür ve örgütsel tasarımdır. Strateji, firmanın ana planını, genel hedeflerini, politika ve programlarını temsil etmektedir. Kurumun felsefesi, tepe yönetimin iş değerleri ve inanışları olarak ele alınırken, kurum kültürü ise örgüt üyeleri tarafından paylaşılan değerler, inanışlar ve varsayımlar olarak tarif edilmektedir. Kurum kültürü firma personelinin neye önem verip vermeyeceğini belirlemekte ve örgütün davranışlarını açıklamaktadır. Kurumsal kimliğin son bileşeni olan örgütsel tasarım ise; bölümlere ayırma, hiyerarşik kademe sayısı, personel sayısı, merkezileşme derecesi, işlerin tasarımı ve içsel sistemler ve süreçlerin bütünü olarak ele alınmaktadır.

Fombrun ve van Riel'e (2004) göre kurumsal kimlik; (a) işgörenlerin firma için merkezi olduğunu düşündükleri özellikleri, (b) firmayı diğer firmalardan ayırt eden özellikleri (işgören gözünden) ve (c) geçmişi ve bugünü geleceğe bağlayan sürekliliği olan özellikleri kapsamaktadır (Barnett ve diğerleri, 2006: 33).

Bromley (2000); kurumsal itibar, kurumsal kimlik ve kurumsal imaj kavramlarını şöyle açıklamaktadır (Wartick, 2002: 376):

- Kurumsal kimlik; ana üyelerin örgütlerini nasıl kavramlaştırdıklarını (köken)
- Kurumsal imaj; bir örgütün kendini dış paydaşlarına nasıl yansıttığını (iletişim)
- Kurumsal itibar; dış paydaşların gerçekte kurumu nasıl kavramlaştırdığının bir sonucunu ifade etmektedir.

Kurumsal itibar; zaman zaman kurumsal imajla eşanlamlı (Dowling, 1993), bazen dışardaki üyelerin kurumsal imaj algısı (Dutton ve diğerleri, 1994) ve kurumsal imajın sadece bir boyutu (Barich ve Kotler, 1991; Mason, 1993) olarak ele alınmaktadır (Caruana, 1997: 110).

Gatewood ve arkadaşları (1993: 424) imajı ve itibarı eşanlamlı gibi görmekte ve imajı dolayısıyla itibar algısını; bireyin belirli bir zamanda erişebileceği bilginin bir fonksiyonu olarak ele almaktadırlar. Benzer şekilde, Macleod (1967: 69) imaj ve itibarı eş anlamlı kullanmakta ve kurumsal imajın (itibarın) birbirlerini etkileyen üç düzeyi olduğunu belirtmektedir. Bu düzeyler aşağıda açıklanmaktadır:

a) Aşinalık: Şirketin ne derece tanındığı ve iyi hatırlandığıyla ilgilidir.

b) Elverişlilik: İnsanların bir şirkete iyi niyetle yaklaşma derecesini ifade etmektedir.

c) Temel özellikler: Bir firmanın alanında öncü olması veya düşük kaliteli mal üreten bir firma olarak tanınması gibi, kamunun firmanın temel özellikleriyle ilgili fikirleridir.

Schwaiger (2004: 50) ise, imaj ve itibar kavramlarının birbirlerinden farklı olduğunu öne sürmektedir. İmajın çağrışıma dayalı özellikleri – çoğu zaman sadece çağrışımsaldır- temsil ettiğini, itibarın ise sadece açıkça görülen özelliklere dayanan tutumsal bir yapı olduğunu savunmaktadır.

Kurumsal imaj ve kurumsal itibar kavramları genellikle iki farklı ancak birbirleriyle önemli ölçüde ilişkili iki kavram olarak görülmektedir. Her iki kavram da sosyal olarak inşa edilmekte ve özellikle müşterilerin firmayla ilgili algılarından türemektedir (Nguyen ve Leblanc, 2001: 227). İmaj ve itibar kavramları kim tarafından bakıldığına göre değişmektedir. Kurum imajı firmayı izleyenlerin firmanın adını veya logosunu gördükleri anda zihinlerinde oluşan görüntüyken, ilişkili bir

kavram olan kurumsal itibar ise paydaşların firmaya yönelik tahminlerini ifade etmektedir (Gray ve Balmer, 1998: 696).

Hem kurumsal itibar hem de kurumsal imaj kavramları firma hakkındaki dışsal algılarla ilgilidir. Kurumsal imaj tüketicilerin zihnindeki firma görüntüsüyken, kurumsal itibar tüketicinin belirli bir özellikle ilgili beklentilerinin karşılanacağına dair firmaya duyduğu güvenin derecesidir. Dolayısıyla, her iki kavram da çeşitli bilgilerin tüketiciler tarafından işlenme sürecinin birikiminden doğan sonuçları ifade etmektedir. Her iki kavramın da duygusal boyutları göz önüne alındığında, tüketicinin firmanın geçmiş eylemlerine veya firmayla yaşadıkları deneyimlere dayanarak oluşturdukları tutumları ve inançlarının kurumsal imaj ve kurumsal itibar algılarını oluşturduğu söylenebilmektedir. Her iki kavram da tüketiciye bir firmanın davranışlarını tahmin edebilmesi yönünde işaretler vermektedir (Nguyen ve Leblanc, 2001: 229).

Aslında kurumsal kimlik, kurumsal imaj ve kurumsal itibar pek çok çalışmada birlikte ele alınmakta ve çoğu zaman birbirlerini tamamlayıcı yapılar olarak görülmektedir. Örneğin; Rao (1994: 30) hem itibarı hem de meşruiyeti örgütsel kimliğin tamamlayıcıları olarak değerlendirmektedir**.**

Chun (2005: 105) ise, imaj ve kimliği itibarın temel unsurları olarak ele almakta; imajı dışardan bakış, kimliği içerden bakış, itibarı ise içsel ve dışsal bakışın toplamı olarak değerlendirerek, her iki unsuru da kapsayan şemsiye bir kavram olarak ele almaktadır.

Barnett ve arkadaşları (2006: 33-34), kurum kimliği, kurumsal imaj ve kurumsal itibar ilişkisini şöyle açıklamaktadır. Kurum kimliği ayırt edici özelliklere vurgu yapmasıyla kurumsal kültürle paralellik göstermektedir. Kurum kültürü yazınında örgüt maddi ve davranışsal sembollerin toplamı ve ilişkili inançlar, değerler ve varsayımlar sistemleri olarak görülmektedir. Buradan yola çıkarak, kurumsal kimliği örgütsel sembollerin toplamı olarak yorumlayabilmek mümkündür. Kurum imajı; iç veya dış paydaşların farklı kurumsal sembollerin toplamına dair genel izlenimlerini ifade ederken, kurumsal itibar ise; gözlemcilerin bir firma hakkındaki yargılarından oluşmaktadır. Bu yargılar kurumsal kimlik veya kurumsal imajdan kaynaklanmakta, ancak genellikle firmanın eylemleri veya hatalarından

doğan tetikleyici bir olayın sonucuna göre oluşmaktadır. Bir firmanın kimliği sabit kalabilirken, imajı ve itibarı dışsal olaylardan fazlasıyla etkilenmektedir.

Genellikle, çarpıcı bir imaj yaratmak değerli bir itibar yaratmaya kıyasla daha hızlı ve kolaydır. Güçlü bir imaj, koordineli bir imaj mühendisliği kampanyasıyla oluşturulabilirken, iyi bir itibarın oluşması için etkili iletişim çabalarından çok daha fazlasına ihtiyaç duyulmaktadır. Bunun için genellikle yıllar süren tutarlı performanslar vasıtasıyla elde edilen saygın bir kimlik gerekmektedir (Gray ve Balmer, 1998: 696).

Gray ve Balmer (1998: 701) ve Cravens ve Oliver (2006: 297) da, kurumsal kimliğin çeşitli iletişim mekanizmaları vasıtasıyla, paydaşların gözünden imaja dönüştürüldüğünü ve zamanla itibari özelliklerin ortaya çıktığını belirtmektedir. Chun (2005: 95-98) ise, kurumsal itibarın temel yapı taşlarını, kimlik (firmanın ne olduğu), arzulanan kimlik (firmanın kendini ne olarak anlattığı) ve imaj (müşterilerin firmayı ne olarak algıladığı) olarak ele almaktadır. İyi bir itibarın bu üç unsur arasındaki uyuma ve algılamalar arasındaki boşlukların giderilmesine bağlı olduğunu savunmaktadır.

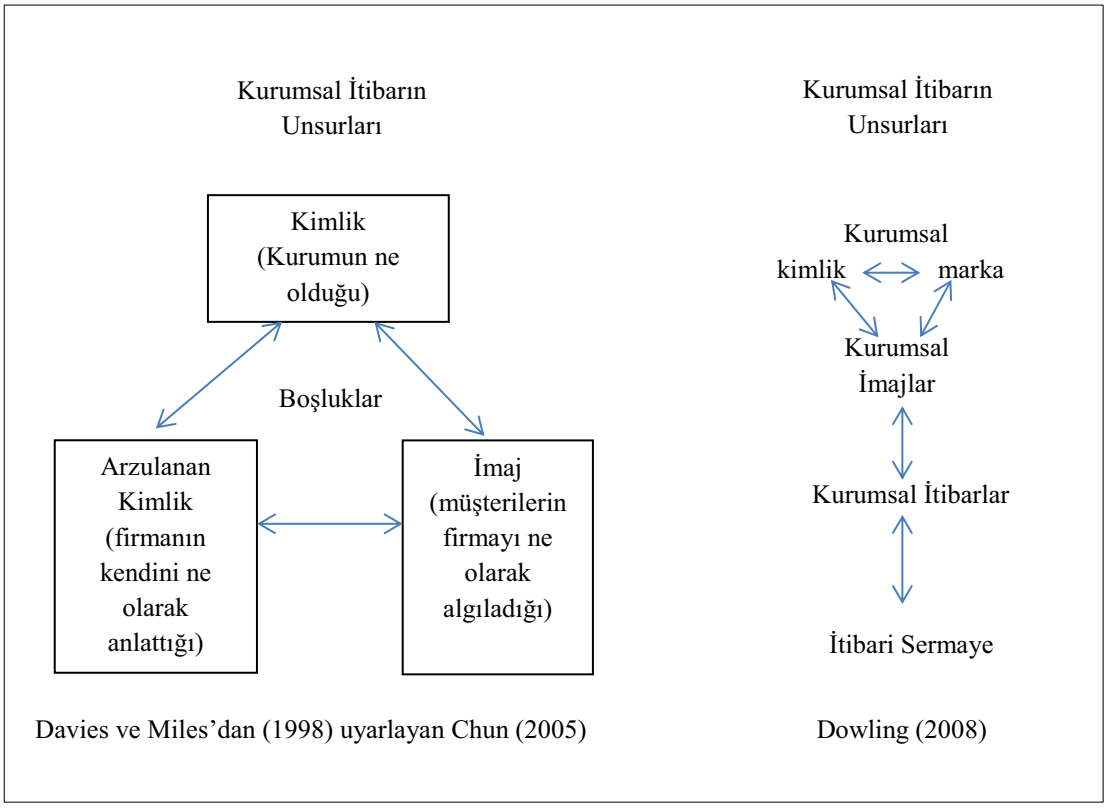
Benzer şekilde, Dowling (2008: 183-184); kurumsal itibar, kurumsal imaj, kurumsal marka, kurumsal kimlik ve itibari sermayeyi aynı ailenin üyeleri olarak görmekte ve bu kavramların birbirleriyle karşılıklı ilişkilerinin olduğunu savunmaktadır. Dowling'e (2008) göre; kurumsal kimlik "firmanın kim olduğu", kurumsal marka "firmanın ne sunduğu", kurumsal imaj "insanların firma hakkında ne düşündüğü", kurumsal itibar "firmanın iyi mi yoksa kötü mü olduğu" ve itibari sermaye ise "kurumun güçlü, zayıf veya değerli olup olmadığı" sorularına cevap vermektedir.

Hem Chun (2005), hem de Dowling (2008) kurumsal itibar, kurumsal kimlik ve kurumsal imaj kavramları arasındaki karşılıklı ilişkilere değinmektedir. Şekil 2'de bu iki araştırmacının kurumsal itibar kavramına yönelik benzer bakış açıları yansıtılmaktadır.

Her ne kadar kurumsal itibar, kurumsal imaj ve kurumsal kimlik gibi kavramlar farklı araştırmacılar tarafından farklı şekillerde ele alınsa da, yaygın olan kanaat bu üç unsurun birbirleriyle ilişkili olduğu yönündedir. Yine de kurumsal itibar, kurumsal kimlik ve kurumsal imaj kavramları arasındaki ilişkileri ortaya

koymak, kurumsal itibar kavramının bu kavramlara benzer ve onlardan farklı yönlerini netleştirmek adına önemlidir.

Şekil 2: Kurumsal İtibarın Unsurları



Kaynak: Chun'dan (2005: 98) ve Dowling'den (2008: 184) uyarlanan kurumsal itibarın unsurları

2.3. KURUMSAL İTİBAR YAKLAŞIMLARI

İtibar, sosyoloji ve oyun teorisi gibi birden fazla disiplinin ilgi alanına girmekte ve bu disiplinlerin her biri kavramı farklı şekillerde tanımlamaktadır (Deephouse, 2000: 1093; Nguyen ve Leblanc, 2001: 228; Chun, 2005: 93; Fombrun ve Van Riel, 1997: 5).

Bazı araştırmacılar (Rao, 1994; Castro ve diğerleri, 2006; Staw ve Epstein, 2000) kurumsal itibarın sosyal olarak inşa edildiğini ve meşrulaşma sürecinin bir çıktısı olduğunu savunmaktayken, bazıları (Schwaiger, 2004: 49) tutumların; öznel, duygusal ve bilişsel tabanlı zihniyetleri ifade ettiği tutumsal bir yapı olarak ele alınmasının gerekli olduğunu söylemektedirler. Diğer bir grup araştırmacı (Weigelt ve Camerer, 1988: 444; Fombrun ve Shanley, 1990: 234; Roberts ve Dowling, 2002:

1079) ise, itibarın; geçmişteki davranışların gelecekte tekrarlanacağına dair beklenti veya sinyaller olarak ele alınmasının gerektiğini ifade etmektedirler.

Daha önce kurumsal itibara yönelik verilen pek çok tanımlama ve bakış açısı, araştırmacıların bu bakış açılarını farklı şekillerde sınıflandırma ihtiyacı hissetmelerine sebep olmaktadır. Her bir sınıflandırma araştırmacıların öznel bakış açılarına göre yapılmış olduğundan, tek bir kurumsal itibar tanımı olmadığı gibi tek bir ekol sınıflandırmasından da bahsedebilmek mümkün değildir. Dolayısıyla, bu bölümde yazında yer alan farklı sınıflandırmalara değinilerek, bu sınıflandırmalara yönelik etraflı bir inceleme yapılacaktır. Ancak bu sınıflandırmalardan bahsetmeden önce, kurumsal itibarın farklı disiplinlerde nasıl ele alındığına dair Fombrun ve Van Riel'in (1997) incelemesine dair kısa bir açıklama yapmak faydalı olacaktır. Fombrun ve Van Riel (1997) kurumsal itibarın; iktisat, strateji, pazarlama, örgütsel, sosyolojik ve muhasebe bakış açılarından ele alındığında değinerek bu bakış açılarını özetlemeye çalışmışlardır.

İktisatçılar, itibarı firmaların davranışlarını açıklayan özellikler veya sinyaller olarak görmektedirler. İtibarın bilgiye dayalı yönü üzerinde durmaktadırlar. Bilgi asimetrisinin kurumsal itibar algısında önemli bir rolü olduğuna ve paydaşların firma hakkındaki bilgilere erişimlerinin farklı olduğuna değinmektedirler. Dolayısıyla iktisatçılara göre itibar işlevseldir, firma ve firmayı oluşturan unsurlarla ilgili paydaşların algılardan oluşmaktadır ve bir firma ve paydaşları arasındaki etkileşimi dengelemektedir (Fombrun ve Van Riel, 1997: 6).

Stratejistler ise; itibarı taklit edilemeyen ve firmanın benzersiz özelliklerinden kaynaklanan bir durum olarak gördüklerinden, rekabet avantajı sağlaması penceresinden değerlendirmektedirler (Fombrun ve Van Riel, 1997: 7).

Pazarlama yazınında itibardan söz edilirken (sıklıkla marka imajı olarak adlandırılmaktadır), dışsal öznelerin (çoğunlukla müşteriler) doğrudan veya dolaylı olarak karşılaştıkları nesnelere (çoğunlukla ürünler) bilişsel ve duygusal anlamlar yüklemesiyle zihinlerinde bu nesnelerle ilgili imgeler oluşması sonucunu doğuran bilgi işleme sürecine odaklanılmaktadır (Fombrun ve Van Riel, 1997: 7).

Örgüt yazınına göre itibar, çalışanların anlamlandırdıkları deneyimlere dayanmaktadır. Kurumsal kültürün ve kurumsal kimliğin önemli bir rolü vardır. Kurumsal kimlik ve kurumsal kültür, örgüt çalışanlarının iş yapma biçimlerinden,

paydaşlarla olan etkileşeme kadar pek çok şeyi etkilemektedir. Güçlü kurumsal kültüre ve kimliğe sahip örgütlerin paydaşların algılarına daha çok önem verdiği görülmektedir (Fombrun ve Van Riel, 1997: 8-9).

Sosyoloji yazınında ise itibar, meşruiyet bağlamında ele alınmakta ve kurumsal çevredeki norm ve beklentilere uygunluğuna göre oluştuğu ifade edilmektedir. Bu doğrultuda, kurumsal çevredeki herhangi bir aktörün kurumsal itibarın oluşumu sürecinde önemli bir rolü bulunmaktadır. Örneğin, firmalarla ilgili değerlendirmeler yapan piyasa analistleri, profesyonel yatırımcılar ve gazeteciler, firmalar ve paydaşları arasındaki bilgi işleme sürecini etkilemektedirler (Fombrun ve Van Riel, 1997: 9).

Muhasebeciler ise gayrı maddi aktiflerin değerlendirilmeleri konusundaki eksikliklere dikkat çekmekte ve gayrı maddi varlıkların hesaplanmasında itibar geliştirme faaliyetleri gibi kapsayıcı bir kalem eklenerek mevcut mevzuatın daha iyi bir hale getirilebileceğini belirtmektedirler (Fombrun ve Van Riel, 1997: 9-10).

2.3.1. Gotsi ve Wilson'ın (2001) Kurumsal İtibar Yaklaşımı

Webster's Revised Unabridged Dictionary'de (1913) itibar: "biri hakkında yapılan tahmin; halkın bakış açısından karakter; bir kişiye, bir şeye veya bir eyleme atfedilen özellik; ün" olarak tanımlanmaktadır (Akt. Gotsi ve Wilson, 2001: 24).

Gotsi ve Wilson (2001: 25) kurumsal itibarla ilgili kavramsal karmaşanın; kurumsal imaj ve kurumsal itibar kavramlarının zaman zaman eşanlamlı, bazen birbirlerinden tamamen farklı, bazen de ilişkili kavramlar olarak ele alınmasından kaynaklandığını öne sürmektedir.

Gotsi ve Wilson'a (2001: 25) göre, kurumsal itibar tanımlaması söz konusu olduğunda iki ana yaklaşım kavramı farklı şekillerde ele almaktadır. Bu yaklaşımlardan ilki kavramı kurumsal imajla eşanlamlı değerlendiren benzetim (analog) yaklaşımı, ikincisi ise; iki kavramı birbirlerinden farklı olarak değerlendiren farklılaştırma yaklaşımıdır. İkinci yaklaşımdaki araştırmacıların büyük çoğunluğuna göre ise, bu iki kavram aynı zamanda birbirleriyle ilişkilidir.

Araştırmacılar ilk yıllarda kurumsal imaj kavramı üzerinde durmakta ancak kurumsal imaj kavramını kurumsal itibarla eşanlamlı gibi kullanmaktadırlar. 1960'lı ve 1970'li yıllarda kurumsal imaj çalışmaları yaygın olduğundan kurumsal imaj

kavramının daha çok kullanılması moda etkisiyle açıklanabilse de, 1990'lara doğru kurumsal itibar çalışmaları da yoğunlaşmış ancak bu dönemde pek çok araştırmacı kavramı kurumsal imajla eşanlamlı olarak değerlendirmeye devam etmiştir (Gotsi ve Wilson, 2001: 25-26).

Farklılaşma yaklaşımından gelenler ise, kavramların benzer şekilde ele alınmasını eleştirmekte ve kavramları ayrımlaştırma gereğini duymaktadır. Bu yaklaşımdan gelenlerin 3 farklı bakış açısı bulunmaktadır. Bunlardan ilki, kurumsal imaj ve kurumsal itibar kavramlarının birbirlerinden tamamen farklı olduğunu ve negatif özelliklerin kurumsal imaj kavramıyla ilgili olduğunu belirtmektedirler. Diğer iki bakış açısı ise, kavramları birbirleriyle ilişkili olarak görmektedir. Farklılaştırma yaklaşımından gelen ikinci görüşe göre kurumsal imaj ve kurumsal itibar kavramları birinci görüşün iddia ettiği gibi tamamıyla farklı değil, birbirleriyle ilişkilidir. Bu görüşteki araştırmacılar, kurumsal itibarı kurumsal imajın bir boyutu olarak değerlendirmekte ve bir firmanın kurumsal itibarının paydaşların gözündeki kurumsal imaj algısını etkilediğini öne sürmektedirler. Üçüncü bakış açısı ise bunun tam tersini iddia etmekte ve kurumsal itibarın paydaşların gözünden oluşan birçok imajdan etkilendiğini iddia etmektedir (Gotsi ve Wilson, 2001: 26-28).

Ancak farklılaştırma yaklaşımının ikinci görüşü, kurumsal imaj ve kurumsal itibar kavramlarının karşılıklı olarak birbirlerini etkileyebileceklerini göz önünde bulundurmamıştır. Ayrıca farklı paydaşların kurumsal imajı farklı algılayabilecekleri gerçeğini de göz ardı etmişlerdir. Bu bağlantılar ise farklılaştırma yaklaşımının üçüncü görüşünden gelen araştırmacılar tarafından ele alınmıştır. Alan yazında kurumsal imaj ve kurumsal itibar kavramlarını birbirleriyle ilişkili olarak gören farklılaştırma yaklaşımının daha çok desteklendiği görülmektedir (Gotsi ve Wilson, 2001: 28). Tablo 5'de Gotsi ve Wilson'ın sınıflandırması özetlenmektedir.

Mevcut yazından yola çıkan Gotsi ve Wilson (2001: 28-29) kurumsal itibarı; "bir paydaşın bir firma hakkında zaman içinde yaptığı genel değerlendirme" olarak tanımlamakta ve beş temel özelliğe sahip olduğunu belirtmektedir. Buna göre kurumsal itibar;

- Dinamik bir kavramdır.
- İnşa edilmesi ve yönetilmesi zaman almaktadır.

- Kurumsal imaj algısını etkilediğinden ve bunun tersi de geçerli olduğundan aralarında karşılıklı bir ilişki bulunmaktadır.
- Rakiplerin olduğu bir ortamda bir firmanın algılanan sıralamasını açığa çıkaran bilişsel bir özelliktir.
- Her paydaşın ekonomik, sosyal ve kişisel geçmişlerine bağlı olarak, her firma için farklılık gösterebilir.

Tablo 5: Gotsi ve Wilson'ın (2001) Kurumsal İtibar Yaklaşımı

Yaklaşımlar	**Kurumsal İtibar ve Kurumsal İmaj İlişkisi**
Benzetim (Bernays, 1977; Boorstin, 1961; Boulding, 1973; Budd, 1969; Crissy, 1971; Enis, 1967; Gates ve McDaniel, 1972; Kennedy, 1977; Martineau, 1958; Schafhauser, 1967 ve sonrası, Abratt, 1989; Alvessson, 1998; Bernstein, 1984; Dichter, 1985; Dowling, 1986, 1993; Dutton vd. 1994)	Kurumsal itibar ≡ Kurumsal imaj
Farklılaştırma	
1. Görüş (Brown ve Cox, 1997; Brown ve Dacin, 1997; Grunig, 1993; O'Sullivan, 1983; Semons, 1998)	Kurumsal itibar ≠ Kurumsal imaj
2. Görüş (Mason, 1993)	Kurumsal itibar ⟹ Kurumsal imaj
3. Görüş (Balmer, 1996, 1997; Bromley, 1993; Fombrun, 1996; Fombrun ve Shanley, 1990; Gray ve Balmer, 1998; Rindova, 1997; Saxton, 1998)	Kurumsal itibar ⟸ Kurumsal imaj

Kaynak: Gotsi ve Wilson, 2001: 25

2.3.2. Chun'un (2005) Kurumsal İtibar Yaklaşımı

Chun (2005: 92) itibarla ilgili kavramsal problemleri itibar paradigması başlığı altında incelemiştir.

Chun'a (2005: 93-95) göre, itibar kavramına bakış açısının; değerlendirici, izlenimsel ve ilişkisel olmak üzere üç yaklaşımdan oluştuğunu söylemek olasıdır. Chun, bu yaklaşım ayrımını odaklandıkları paydaş gruplarına göre yapmaktadır. Değerlendirici ve izlenimsel yaklaşımlar tek bir paydaş grubunun çıkarları üzerinden

hareket ederken, ilişkisel yaklaşım paydaş teorisini dikkate alarak farklı paydaşların farklı beklentileri olduğu varsayımından hareket etmektedir.

Değerlendirici yaklaşım itibarı firmanın finansal değerine veya kısa dönemli finansal performansına göre ölçmekte ve itibarı rekabet avantajı sağlayan gayrı maddi bir varlık olarak ele almaktadır. Bu akımın üzerinde durduğu paydaş grupları ise; hissedarlar ve yatırım danışmanları gibi iç paydaşlardır (Chun, 2005: 93).

1990'lardan itibaren ise, firmaların uzun dönemli finansal performansını etkileyeceği düşüncesiyle, paydaşların firmalarla kurduğu duygusal ilişkiler ilgi odağı olmaya başlamıştır. Dış paydaşlar ve itibarın finansal olmayan özellikleriyle ilgilenen araştırmacılar ise, ya izlenimsel ya da ilişkisel yaklaşıma dahildir. İmaj, kimlik ve kişilik gibi terimler izlenimsel yaklaşımda sıklıkla kullanılmaktadır. Bu yaklaşımdaki araştırmacılar itibarı finansal performanstan ziyade ilgili paydaşların algıları ve izlenimlerine göre ölçmeye çalışmışlardır. Pazarlama ve örgütsel davranış yazınındaki çalışmalar bu gruba girmektedir. Bu çalışmalarda ele alınan paydaşlar, çoğunlukla işgörenler ya da müşterilerdir (Chun, 2005: 93). Örneğin, bu yaklaşımdan gelen Brown ve arkadaşları (2005) itibarı, firma dışındaki bir bireyin firmayla kurduğu zihinsel ilişkiler kümesi olarak tanımlamaktadır (Chun, 2005: 93).

İlişkisel yaklaşımdan gelen araştırmacılar ise, çoklu paydaş anlayışından yola çıkarak itibarı, bütün paydaşların algılarının bir toplamı veya sentezi olarak ele almaktadır. Dolayısıyla bir örgütün birden fazla itibarı olduğunu savunmaktadırlar. Bu yaklaşımdaki araştırmacılar imaj kavramını firma dışındakilerin algısı olarak değerlendirmekteyken, itibarı ise iç ve dış paydaşların algılarını kapsayan bir kavram olarak ele almaktadırlar (Chun, 2005: 94-95).

İzlenimsel yaklaşımı savunanlar itibarı tek bir paydaşın firmayla ilgili algılarının toplamı olarak ele alırken, ilişkisel yaklaşımı savunanlar ise bütün paydaşların algılarının kollektif yansıması olarak ele almaktadırlar (Chun, 2005: 95).

Chun'a göre itibarın temel yapı taşları, kimlik (firmanın ne olduğu), arzulanan kimlik (firmanın kendini ne olarak anlattığı) ve imajdan (müşterilerin firmayı ne olarak algıladığı) oluşmaktadır. İyi bir itibar bu üç unsur arasındaki uyuma ve algılamalar arasındaki boşlukların giderilmesine bağlıdır (Chun, 2005: 95-98).

Chun'un itibar paradigması olarak ele aldığı yaklaşımlar Tablo 6'da gösterilmektedir.

Tablo 6: Chun'un (2005) Kurumsal İtibar Yaklaşımı

Yaklaşımlar	**Kilit Paydaşlar**		**Odak Nokta**	**Örnek Araştırmalar**
Değerlendirici Yaklaşım: Finansal başarının değerlendirilmesi olarak itibar	Tek paydaş grubu (yatırımcı veya yönetici)		Yatırımcı Davranışı	Fryxell ve Wang (1994)
			Genel müdürlerin fikirlerine dayalı sıralama	Yıllık Fortune Araştırmaları
			Yatırımcı	Srivastava vd. (1997)
			İtibarı finansal/stratejik performansla ilişkilendirmek	Fombrun ve Shanley (1990); Weigelt ve Camerer (1988)
İzlenimsel Yaklaşım: Kurumla ilgili genel izlenim olarak itibar	Genelde tek paydaş grubu	Pazarlama	İmaj/kurum kimliği	Abratt (1989); Bromley (1993); Balmer (1997); Brown vd. (2005); Dowling (1993)
			İtibarı tüketicinin satın alma niyetiyle ilişkilendirmek	Yoon vd. (1993)
			Müşterilerin kurum ve satış temsilcisi imajına bakış açısı	Weiss vd. (1999)
		Örgütsel Davranış	İşgören özdeşleşmesi ve itibar ilişkisi	Dutton vd. (1994) Dutton ve Dukerich (1991)
			Yönetimin imaj ve kimlik algısı	Gioia ve Thomas (1996)
		Medya	Medya koverajının uygunluğu ve itibar ilişkisi	Deephouse (2000)
İlişkisel Yaklaşım: İç ve dış paydaşların bakış açıları arasındaki açıklıklar bağlamında itibar	Birden çok paydaş bakış açısının kıyaslanması (Genellikle iç ve dış paydaş bakış açıları karşılaştırılmaktadır)		Tüm paydaşların genel olarak ele alınması	Fombrun (1996); Post ve Griffin (1997)
			Kurumsal itibarın iç (kimlik) ve dış (imaj) bakışlarını birleştirmek	Hatch and Schultz (2001); Davies ve Chun (2002); Chun ve Davies (2006)
			İtibar (dışsal bakış) ve kimliği (içsel bakış) ilişkilendirmek	Fiol ve Kovoor-Misra (1997)

Kaynak: Chun, 2005: 94.

2.3.3. Rindova, Williamson, Petkova ve Sever (2005) Yaklaşımı

Rindova ve arkadaşlarına (2005: 1033-1034) göre, kurumsal itibar kavramı söz konusu olduğunda iki farklı yaklaşımdan bahsedilebilir. Bunlardan ilki, gözlemcilerin bir firmanın belli bir özelliğine dair beklentilerini veya tahminlerini tanımlaya çalışan iktisadi perspektiftir. Bu bakış açısına göre itibar, firmaların geçmiş eylemleri vasıtasıyla paydaşlarına gönderdikleri gerçek özelliklerine dair sinyallerden oluşmaktadır. İkinci perspektif ise, itibarı küresel bir izlenim olarak gören kurumsallaşma yaklaşımıdır. Bu yaklaşım kurumsal itibarı, bir topluluğun – bir veya birden fazla paydaş grubunun - bir firmayı nasıl algıladığı olarak değerlendirmekte ve itibarın örgütsel bir alanda etkileşim halinde bulunan aktörler arasındaki bilgi alışverişi ve sosyal etkinin bir sonucu olarak ortaya çıktığını öne sürmektedir.

Rindova ve arkadaşları (2005: 1034) bu iki yaklaşımın farklı bakış açılarını itibarın iki boyutu olarak ele almaktadırlar. İktisadi perspektifin itibar tanımından yola çıkarak, algılanan kalite boyutunu paydaşların bir firmanın belirli bir özelliğini nasıl değerlendirdikleriyle ilişkilendirmektedir. Kurumsallaşma teorisi ise itibarı kollektif farkındalık ve tanınma olarak ele aldığından, şöhret itibarın ikinci boyutu olarak değerlendirilmektedir.

İktisadi perspektiften bakan araştırmacılara göre itibar konusundaki belirsizlikler rekabet içindeki firmalar ve paydaşları arasındaki bilgi asimetrisinden kaynaklanmaktadır. Firmalar, gerçek özelliklerini açığa çıkaracak seçimler yaptığında bilgi asimetrisini ve buna bağlı olarak pazar belirsizliğini düşürmektedir. Dolayısıyla bu bakış açısına göre itibar, paydaşların firmaların ürünlerinin kalitesi konusundaki şüpheleri azaltmaktadır (Rindova ve diğerleri, 2005: 1034).

Kurumsallaşma perspektifinden bakan araştırmacılara göre ise; firmaların gerçek özellikleriyle ilgili belirsizlikler, örgütsel sahadaki kurumsal aracılar ve yüksek statülü aktörler gibi bilgiye erişimi olan ve bunu yayabilen çeşitli aktörler arasındaki bilgi alışverişi vasıtasıyla azalmaktadır. Firmaların paydaşları bu aktörlerin firmalarla ilgili değerlendirmelerine güvenmekte ve yakından takip etmektedirler. Dolayısıyla, üçüncü tarafların yaptıkları değerlendirmeler bazı firmaları diğerlerinden daha ünlü hale getirmektedir. Dolayısıyla bu görüşe göre firmanın örgütsel sahasında rakiplerine kıyasla paydaşlar tarafından ne derece

tanındığı önem taşımakta ve bu sebeple itibarın önemli bir boyutu olarak ele alınabileceği söylenebilmektedir (Rindova ve diğerleri, 2005: 1034-1035). Tablo 7'de Rindova ve arkadaşlarının kurumsal itibar yaklaşımları gösterilmektedir.

Tablo 7: Rindova ve Diğerlerinin (2005) Kurumsal İtibar Yaklaşımı

Araştırma Alanı	**İtibar Tanımı**	**Yapıyla Eşleştirilen Algı Tipi**	**Örnek Çalışmalar**
Yönetim Ekonomisi/Oyun Teorisi Perspektifi	Firmanın geçmiş eylemlerine dayanarak bu firmaya atfedilen özellik veya özellikler seti	İlişkili özelliklerin değerlendirilmesi	Weigelt ve Camerer (1988) Hayward ve Boeker (1998) Stuart (2000)
	Bir gözlemcinin, bir aktörün belli bir davranışı sergileyeceğine dair izlenimi	İlişkili özelliklerin değerlendirilmesi	Clark ve Montgomery (1998)
Kurumsal Perspektif	Küresel algı; halkın zaman içinde bir firmayla ilgili birikmiş yargıları	Kolektif bilgi ve tanınma	Fombrun ve Shanley (1990) Roberts ve Dowling (2002)
	Paydaşların bir firmaya yönelik bilgisi ve duygusal reaksiyonları (hoşlanma, saygı)	Kolektif bilgi ve tanınma	Hall (1992) Fombrun (1996) Deephouse (2000)
Pazarlama Perspektifi	Bir firmanın kendisi ve markalarıyla ilgili oluşturduğu farkındalık düzeyi; ün	Kolektif bilgi ve tanınma	Hall (1992) Shamsie (2003)
İktisat	Tüketicilerin bir firmanın ürünlerinin kalitesi hakkındaki inanç ve algıları	İlişkili özelliklerin değerlendirilmesi	Shapiro (1982, 1983) Allen (1984)
	Sektör içindeki bir rakibin sektör içindeki firmanın beklenen şekilde davranma olasılığına dair algısı	İlişkili özelliklerin değerlendirilmesi	Kreps ve Wilson (1982) Milgrom ve Roberts (1982)
Sosyoloji	İlgili kamunun bir aktör hakkında ne bildiğine dayanan, bu aktörün özellikleri veya başarıları hakkındaki en geçerli kolektif uzlaşısıdır	Kolektif bilgi ve tanınma	Lang ve Lang (1988) Camic (1992)
	Bir aktörün geçmiş eylemlerine dayanarak bu aktörlerle ilişkilendirilen özellik veya atıflardır	İlişkili özelliklerin değerlendirilmesi	Raub ve Weesie (1990) Kollock (1994)
Pazarlama	Bir varlığın bir özelliğinin zaman içindeki tutarlılığına yönelik tahmindir	İlişkili özelliklerin değerlendirilmesi	Herbig ve Milewicz (1995)
	Tüketicilerin, belirli bir ürün veya markayı üreten firma hakkındaki izlenimleri	Kolektif bilgi ve tanınma	Goldberg ve Hartwick (1990)
	Bir firmayla yaşanan geçmiş etkileşimlere dayalı algı ve inançlardır	İlişkili özelliklerin değerlendirilmesi	Campbell (1999) Prabhu ve Stewart (2001)
	Kamunun saygı veya hürmeti	Kolektif bilgi ve tanınma	Weiss, Anderson, ve Maclnnis (1999)

Kaynak: Rindova ve diğerleri, 2005: 1036.

2.3.4. Diğer Sınıflandırmalar

Yukarıda ayrıntılı olarak ele alınan sınıflandırmalar dışında, kurumsal itibar yaklaşımlarına yönelik farklı bakış açılarını yansıtan başka çalışmalar da bulunmaktadır.

Love ve Kratz (2009: 315-317) kurumsal itibara genel olarak üç bakış açısının olduğunu ifade etmektedir. İtibarı örgütsel karakter olarak ele alanlar, gözlemcilerin firmaları arzuladıkları karakter özelliklerine göre yorumladıklarını belirtmektedir. Bu görüşten gelenler; örgütleri amaçlı sosyal varlıklar olarak değerlendirmekte, mübadele açısından bakarak gözlemcilerin firmanın gelecekteki eylemlerinin tahmin edilmesi konusunda güvenilir olmasına göre firmaya hayranlık duyduklarını belirtmekte ve fırsatçı yaklaşımların hoş karşılanmadığını öne sürmektedir.

Sembolik uyum perspektifi, daha çok yeni kurumsal kuramla ilişkili olarak görülmekte ve firmanın dışsal ve sosyal olarak inşa edilen standartlara uymasına göre itibarın değerlendirildiğini öne sürmektedir. Örgütler yapılarını ve uygulamalarını sektör düzeyindeki baskılara göre şekillendirmekte ve bu bağlamda meşruiyet ve destek kazanmaktadır.

Üçüncü görüş ise; kurumsal itibarı firmanın somut çıktılarına göre değerlendiren teknik etkinlik perspektifidir. Bu görüşe göre paydaşların algıları, finansal performans ve ürün ve hizmetlerin kalitesi gibi çıktılara dayalı olarak şekillenmektedir.

Alan yazında sadece bakış açılarına ve hangi disiplinden olduklarına göre değil, kullanılan tanımlara göre de kurumsal itibara bakış açılarını sınıflandıran çalışmalar mevcuttur. Barnett, Jermier ve Lafferty'nin (2006) tanımsal farklılıklardan yola çıkarak yaptıkları sınıflandırma buna örnek olarak verilebilir.

Barnett ve arkadaşlarına (2006: 32) göre; kurumsal itibar tanımları 3 grupta toplanmaktadır. Kurumsal itibar; (a) bir farkındalık durumu olarak, (b) bir değerlendirme şeklinde ve (c) bir varlık olarak tanımlanmaktadır.

Farkındalık tanımlamaları yapan gruptaki araştırmacılar kurumsal itibarı; paydaşların firma hakkında yargıda bulunmadıklarını, firma hakkında genel bir farkındalıklarının olduğu şeklinde yorumlamaktadır. Bu gruptakiler itibarı tanımlarken algı terimini kullanmaktadırlar. Kurumsal itibar paydaşların toplam, net,

küresel, kolektif vb. algıları olarak tanımlanmaktadır. Aynı zamanda, kurumsal itibar bilgi ve duyguların temsilcisi olarak da görülmekte ki, bu da firma hakkındaki farkındalığa işaret etmektedir (Barnett ve diğerleri, 2006: 32).

Tablo 8: Bir Bütün Olarak Kurumsal İtibara Farklı Yaklaşımlar

ÇALIŞMALAR	EKOLLER		TEMEL VARSAYIMLARI
Gotsi ve Wilson (2001)	Benzetim (Analog)		Kurumsal itibar ve kurumsal imaj kavramları birbirinin dengidir
	Farklılaştırma	1. Görüş	Kurumsal imaj ve kurumsal itibar kavramları birbirlerinden tamamıyla farklıdır
		2. Görüş	Kurumsal imaj kurumsal itibarı kapsamaktadır
		3. Görüş	Kurumsal itibar kurumsal imajı kapsamaktadır
Chun (2005)	Değerlendirici		İtibar, finansal başarının değerlendirilmesi olarak ele alınmaktadır
	İzlenimsel		İtibar, kurumla ilgili genel izlenimleri ifade eder
	İlişkisel		İtibar, iç ve dış paydaşların bakış açıları arasındaki açıklıklardan doğar
Rindova, Williamson, Petkova ve Sever (2005)	İktisadi		İtibar, firmaların geçmiş eylemleri vasıtasıyla paydaşlarına gönderdikleri gerçek özelliklerine dair sinyallerden oluşmaktadır
	Kurumsallaşma		İtibar, örgütsel bir alanda etkileşim halinde bulunan aktörler arasındaki bilgi alışverişi ve sosyal etkinin bir sonucu olarak ortaya çıkmaktadır
Love ve Kratz (2009)	Örgütsel Karakter		Gözlemciler, firmaları arzuladıkları karakter özelliklerine göre yorumlamaktadırlar ve örgütler amacı olan sosyal varlıklar olarak görülmektedirler
	Sembolik Uyum		İtibar, firmanın dışsal ve sosyal olarak inşa edilen standartlara uymasına göre değerlendirilmektedir
	Teknik Etkinlik		Paydaşların algıları, finansal performans ve ürün ve hizmetlerin kalitesi gibi çıktılara dayalı olarak şekillenmektedir
Barnett, Jermier ve Lafferty (2006)	Farkındalık		Paydaşların firma hakkında yargıda bulunmadığı, firma hakkında genel bir farkındalıklarının olduğu düşünülmektedir
	Değerlendirme		İtibar bir değerlendirme olarak ele alınmaktadır
	Varlık		İtibar değerli bir kaynak olarak görülmekte ve gayrı maddi, finansal veya ekonomik bir varlık olarak ele alınmaktadır

İkinci grup itibarı bir değerlendirme olarak ele almaktadır. İtibarı tanımlarken kullandıkları kelimeler ve dil, itibarı paydaşların firmanın statüsü hakkındaki değerlendirmeleri olarak ele aldıklarını göstermektedir. Kurumsal itibarı; değerlendirme, ölçme, tahmin ve yargı gibi kelimelerle ifade etmektedirler. Buna ek

olarak, saygı ve firmanın çekiciliği gibi kavramların yanı sıra, fikir ve görüş gibi doğasında yargısal bir anlam barındıran kelimelere de sıklıkla başvurmaktadırlar (Barnett ve diğerleri, 2006: 32-33).

Üçüncü grup tanımlamalarda ise kurumsal itibar, firma için önemi olan ve değerli bir şeyi ifade etmek için kullanılmaktadır. İtibar değerli bir kaynak olarak görülmekte ve gayrı maddi, finansal veya ekonomik bir varlık olarak ele alınmaktadır. Dolayısıyla firmanın itibarının gerçek bir değeri olduğu üzerinde durmaktadırlar (Barnett ve diğerleri, 2006: 33).

Görüldüğü üzere kurumsal itibar yaklaşımlarından söz edildiğinde tek bir bakış açısına göre değerlendirme yapmak pek de doğru olmayacaktır. Yukarıda açıklanan sınıflandırma çalışmalarının her biri kendi içerisinde bir özgünlük taşımaktadır. Tablo 8'de bu yaklaşımlar özetlenmektedir.

2.4. KURUMSAL İTİBARIN ÖLÇÜMÜ

Kurumsal itibarın yönetilebilmesi için öncelikle ölçülebilmesi gerekmektedir (Gardberg ve Fombrun, 2002: 303). İtibar ölçümünün doğru bir şekilde yapılması ise, sadece firmanın paydaşlarını temsil edebilecek bir örneklem ve kavramsal olarak ilişkili bir kriter setiyle mümkündür (Fombrun, 1998: 338). Ancak, kurumsal itibarın temel özellikleri olan; nedensel belirsizliği, sosyal karmaşıklığı, zaman içindeki birikimi ve geçmişe bağlılığı itibarı örtük ve soyut bir kavram yapmakta ve ölçümünü zorlaştırmaktadır (Castro ve diğerleri, 2006: 362).

Ekonomik göstergelerin itibar üzerinde önemli etkileri olduğu düşünülse de, itibar sadece finansal performansa göre değerlendirilmemeli (Caruana, 1997: 109), firmaların farklı paydaşlara hizmet ettikleri ve bu paydaşların her birinin farklı değerlendirme kriterleri bulunduğu da dikkate alınmalıdır (Fombrun ve Shanley, 1990: 234). Dolayısıyla itibarın ölçülmesinde; müşteriler, çalışanlar ve tedarikçiler gibi paydaşların da araştırmaların katılımcıları arasında yer almaları gerekmektedir (Roberts ve Dowling, 2002: 1091).

Fombrun (1998: 338) kurumsal itibarın kavramsal yapısını ortaya koymak için yapılacak çalışmalarda iki önemli noktaya dikkat edilmesi gerektiğini belirtmektedir. Bu noktalar;

- Kollektif yargıyı göstermesi için birden çok paydaş grubunun olduğunun dikkate alınması ve
- Değerlendirmeyi hangi paydaşların yaptığı göz önünde bulundurularak, birbirlerinden farklı ancak birbirleriyle örtüşen finansal ve sosyal kriterlerin belirlenmesidir.

Alan yazın incelendiğinde kurumsal itibarı ölçmeye yönelik pek çok çalışma yapıldığı görülmektedir. Bu çalışmalardan bazıları, kurumları ağırlıklı olarak finansal performans kriterlerine göre değerlendirerek firmaları kıyaslama amacı taşıyan sıralamalardır. Diğer çalışmalar ise; ya yazında var olan itibar ölçeklerinin nitel araştırmalarla desteklenerek revize edilmesi ve yeni boyutlara göre değerlendirilmesiyle yapılmakta, ya da farklı disiplinlerde kurumsal itibarla ilişkili olarak görülebilecek diğer kavramlara ait ölçeklerin uyarlanmasıyla gerçekleştirilmektedir.

2.4.1. Sıralama Bazlı Ölçümler

Yönetim ve bilim camiasının kurumsal itibara ilgisinin yoğunlaşmasında Fortune, Financial Times, Asian Business and Manager Magazin gibi dergi ve gazetelerin yaptıkları itibar sıralamalarının önemli bir etkisi olduğu düşünülmektedir (Gardberg ve Fombrun, 2002: 305).

İtibar sıralamaları firmaların performanslarını farklı kriterlere göre ölçmekte ve doğrudan firmaları birbirleriyle kıyaslamaktadır. İtibar sıralamaları, paydaşların firmalarla ilgili farklı algılarına yönelik bir manifesto niteliği taşımakta ve rekabet avantajını etkilemektedir (Rindova ve Fombrun, 1999: 700).

İtibar sıralamaları, kurumsal aynalara benzemektedir. Daha açık bir ifadeyle, kurumlar itibarlarını bu sayede gözlemleyerek, mikro kültürlerini ve maddi kaynaklarını paydaşlar tarafından belirlenen başarı tanımının gereklerini yerine getirecek şekilde uyumlaştırmaktadır (Rindova ve Fombrun, 1999: 700-701).

Kurumları itibarlarına göre sıralamaya dayanan pek çok ölçek bulunmaktadır (bkz. Fombrun, 1998; Fombrun ve diğerleri, 2000). Geçmişten günümüze, çeşitli dergi ve gazeteler, sivil toplum kuruluşları, şirketler vb. pek çok kuruluş firmaların kurumsal itibarlarını belirlemek adına farklı kriterler üzerinden hareket etmekte ve itibar sıralamaları yayınlamaktadırlar. Her ne kadar bu kurumlardan bazıları çeşitli

sebeplerden ötürü yayınlarına son vermişlerse de, bunların yerini yenileri almaktadır. Dolayısıyla aşağıda, geçmişte kullanılan veya yeni yeni ortaya çıkan endekslerden ziyade, uzun yıllardan beri bu sıralamaları yapan ve yaygın kabul gören endeksler ele alınacaktır.

2.4.1.1. Fortune İtibar Endeksi (AMAC ve WMAC)

Fortune dergisi, 1984 yılında (1983 verilerine dayanarak) ilk kez yayınladığı "Amerika'nın En Çok Hayranlık Duyulan Şirketleri" (America's Most Admired Companies) sıralamasından beri her yıl kurumsal itibar sıralamaları yayınlamaktadır. Bu sıralama, yöneticilerin ve analistlerin 8 kritere göre sektörlerindeki bütün firmaları değerlendirmeleri sonucu oluşmakta ve bireysel cevapların toplanmasıyla firmaların toplam skorları belirlenmektedir. Söz konusu bu sekiz kriter; ürün veya hizmet kalitesi, yönetimin kalitesi, yenilikçilik, uzun dönemli yatırım değeri, finansal istikrar, yetenekli insanları çekme, geliştirme ve elde tutabilme kabiliyeti, çevresel ve sosyal sorumluluk ve kurumsal varlıkların akılcı kullanımı olarak sıralanmaktadır (Fombrun, 1998: 328; Fombrun ve diğerleri, 2000: 243-244; Staw ve Epstein, 2000: 535-536). Küreselleşmenin önem kazanmasıyla birlikte, küresel iş yapabilme etkinliği dokuzuncu kriter olarak Fortune ölçümüne dahil edilmiştir. "Dünya'da En Çok Hayranlık Duyulan Şirketler" (WMAC) sıralaması 1997 yılından itibaren, "Amerika'nın En Çok Hayranlık Duyulan Şirketleri" (AMAC) sıralaması ise 2001 yılından itibaren Hay Group işbirliğinde yapılmaktadır (www.fortune.com; www.haygroup.com).

2.4.1.2. Management Today Britanya'nın En Çok Hayranlık Duyulan Şirketleri (BMAC) Endeksi

Management Today, 1989 yılından beri her yıl Britanya'nın en büyük şirketlerinin itibarına yönelik sıralamalarını yayınlamaktadır. Başlangıçta; yönetim kalitesi, finansal istikrar, yetenekli insanları çekme, geliştirme ve elde tutabilme kabiliyeti, pazarlama kalitesi, çevresel ve sosyal sorumluluk ve kurumsal varlıkların kullanımı olmak üzere 6 kritere göre oluşturulan endeks (Fombrun, 1998: 329), bugünkü haliyle; ürün ve hizmet kalitesi, yenilikçilik ve uzun dönemli yatırım değeri olmak üzere 3 kriterin de eklenmesiyle 9 kriterin ölçüldüğü bir yapı halini almıştır. BMAC, Management Today ve Leeds Business School işbirliğiyle

oluşturulmaktadır. Dokuz kritere göre hazırlanan ölçek işletme yöneticilerine gönderilerek, sektördeki rakiplerine bu kriterlere göre 0 ve 10 arasında bir değer vermeleri istenmektedir. Elde edilen verilere göre hem genel itibar bazında hem de her bir kritere göre kurumlar sıralanmaktadır (http://www.managementtoday.co.uk).

2.4.1.3. Harris-Fombrun İtibar Katsayısı (Reputation Quotient) ve Reputation Institute

Fombrun ve arkadaşları (2000) tarafından geliştirilen İtibar Katsayısı Modeli, belki de itibar ölçümleri arasında hem akademik hem de yönetim dünyasında en çok kabul gören ölçme modelidir. Bu sebeple İtibar Katsayısı Modelini detaylıca açıklamak faydalı olacaktır.

İtibar Katsayısı 1998 yılında başlayan bir projedir. Fombrun (1998: 334-335), mevcut itibar ölçümlerini inceledikten sonra itibar değerlendirmelerinde kullanılan kriterleri altı başlık altında toplamıştır. Bunlar; finansal performans, ürün kalitesi, çalışma koşulları, sosyal sorumluluk, çevresel performans ve örgütsel konular (fırsat eşitliğine, farklılıkların yönetimine ve etik davranışa önem verme gibi) olarak sıralanmaktadır.

Daha sonra ise Fombrun, Gardberg ve Sever (2000), mevcut ölçek maddeleri ve literatürden yola çıkarak ve gerekli elemeleri yaptıktan sonra 8 grupta toplanan 32 maddelik bir ölçek elde etmiştir. Ölçeği sınamak için yapılan pilot çalışmada elde edilen sonuçların tatmin edici olmaması sebebiyle, kurumsal itibarın boyutlarını belirleyebilmek adına odak grup görüşmelerine başvurulmuştur.

Özetle, yapılan bir dizi odak grup görüşmesi ve ortaya çıkarılan ölçeklerin geçerliliğini sınamak adına sonrasında yapılan pilot testler sonucunda 6 boyutlu ve 20 maddelik İtibar Katsayısı geliştirilmiştir. Bu çalışmaya göre kurumsal itibar; duygusal cazibe, ürün ve hizmetler, vizyon ve liderlik, çalışma ortamı, sosyal ve çevresel sorumluluk ve finansal performans olmak üzere altı boyuttan oluşmaktadır (Fombrun ve diğerleri, 2000: 250). Bu boyutlar aşağıda kısaca açıklanmaktadır (Fombrun ve Gardberg, 2000: 13):

- Duygusal Cazibe: Firmanın ne derece sevildiği, hayranlık ve saygı duyulduğudur.
- Ürün ve Hizmetler: Ürün ve hizmetlerin; kalite, inovasyon, değer ve güvenilirliklerine yönelik algılardır.

- Finansal Performans: Firmanın karlılığı, geleceği ve risk durumuyla ilgili algılardır.
- Vizyon ve Liderlik: Firmanın ne derece açık bir vizyon ve güçlü bir liderlik sergilediğiyle ilgili algılardır.
- Çalışma Ortamı: Firmanın ne kadar iyi yönetildiği, bu firma için çalışmanın nasıl olduğu ve çalışanlarının kalitesine ilişkin algılardır.
- Sosyal Sorumluluk: Toplumla, çevresiyle ve çalışanlarıyla ilişkilerinde ne derece iyi bir vatandaş (citizen) olduğuna yönelik algılardır.

2005-2006 yıllarında ise İtibar Katsayısı Modeli evrimleştirilerek RepTrak Modeli ortaya atılmıştır. Bu yeni model kurumsal itibarı toplam 23 maddelik 7 boyutlu bir ölçekle ölçmektedir. Diğer altı boyut itibar katsayısı modeliyle aynı olmakla birlikte, yenilikçilik 7. boyut olarak kurumsal itibarın boyutları arasına eklenmiştir (http://www.reputationinstitute.com).

2.4.2. Diğer Ölçümler

Firmaları belli kriterlerden alınan skorlara göre kıyaslayan sıralama yaklaşımının dışında, kurumsal itibarı ölçmeye yönelik daha farklı yaklaşımlar da bulunmaktadır. Berens ve Van Riel (2004) kurumsal itibar ölçümlerine yönelik yaptıkları yazın taraması sonucunda üç ana akımın olduğunu belirtmektedirler. Bu akımlardan ilki, kurumsal itibarı farklı paydaşlarının beklentilerine göre ölçmeye çabalayan toplumsal beklentiler akımıdır. Bu gruptaki çalışmalarda, kurumsal itibar ürün hizmet kalitesi, çevreye verilen zarar, iyi bir finansal performans gibi paydaşların farklı beklentilerine göre ölçülmektedir (Berens ve Van Riel, 2004: 162-168). Bu akıma verilebilecek en güzel örnekler ise bir önceki bölümde sıralama bazlı ölçekler olarak ele aldığımız endekslerdir.

İkinci ana akım ise, örgütlerin itibarını bireysel kişilik özelliklerine dayalı olarak ölçmektir. Örneğin Spector (1961) kurumsal itibarı, diğer kişilik envanterlerinden aldığı maddelere dayanarak ölçmüştür (Berens ve Van Riel, 2004: 169-172). Davies ve arkadaşları (2003: 148-158) da benzer bir yaklaşımla kurumsal itibarı ölçmek için kurumsal kişilik ölçeği oluşturmuşlardır. Ölçek; hoşluk, girişkenlik, yetkinlik, gaddarlık, şıklık, resmi olmama ve maçoluk olmak üzere 7 ana boyutu içermektedir.

Berens ve Van Riel'e (2004: 172) göre, üçüncü ana akım ise güvene dayalı itibar ölçümleridir. Bu akıma göre itibar, aktörlerin sözlerini yerine getireceğine dair beklenti olarak ele alınmaktadır. Dürüstlük, güvenilirlik, yardımseverlik gibi maddelerle ölçülmeye çalışılmaktadır.

Daha önce de sözü edildiği üzere, alan yazında kurumsal itibarı tüm paydaşların algılarının toplamı olarak ölçen çalışmalara ağırlık verilmiştir. Son yıllarda ise, tek bir paydaş grubuna ve farklı iş faaliyetlerine yönelik spesifik ölçekler de oluşturulmaya başlanmıştır. Walsh'un çalışma arkadaşlarıyla yaptığı ölçek geliştirme araştırmaları buna verilebilecek güzel bir örnektir.

Walsh ve Beatty (2007) hizmet sektörüne yönelik müşteri tabanlı kurumsal itibar ölçeğini geliştirmişlerdir. Bu ölçek; ürün ve hizmet kalitesi, iyi işveren olma, müşteri yönelimi, güvenilir ve finansal olarak güçlü şirket ve sosyal ve çevresel sorumluluk olmak üzere 5 boyuttan ve toplamda 28 maddeden oluşmaktadır. Walsh ve arkadaşları (2009a) müşteri tabanlı kurumsal itibar ölçeğinin 15 maddelik kısa bir versiyonunu da oluşturmuşlardır. 2015 yılında ise Walsh ve arkadaşları; etik, ilişkisel eşitlik, uzmanlık ve müşteri merkezlilik olmak üzere 4 boyuttan oluşan 18 maddelik yeni bir müşteri (bu çalışmada ele alınan müşteriler birbirleriyle iş yapan işletmelerdir) tabanlı kurumsal itibar ölçeği geliştirmişlerdir. Bu boyutlar aşağıda kısaca açıklanmaktadır (Walsh ve diğerleri, 2015: 178):

- Etik; müşterilerin, firmanın müşterilerle olan ilişkilerinde dürüst davranma kabiliyetine yönelik algılarıyla ilgilidir.
- İlişkisel Eşitlik; müşterilerin, firmanın içinde bulunduğu sektör ve toplumla iyi ilişkiler kurma ve bunu sürdürme kabiliyetine dönük algılarıdır.
- Uzmanlık; müşterilerin, firmanın müşteri ihtiyaçlarını karşılama yetkinliği ve uzmanlığına yönelik algılarıdır.
- Müşteri merkezlilik; müşterilerin, firmanın müşteri ilişkilerini önemseyerek sorunları çözümsüz bırakmayacağına yönelik algılarıdır.

Müşteri tabanlı kurumsal itibar ölçeğine yönelik çalışmalar, kurumsal itibarın farklı paydaşlar ve bu paydaşların farklı beklentileri söz konusu olduğunda farklı unsurlardan oluşabileceğini göstermesi bakımından önem taşımaktadır. Nitekim Walsh ve arkadaşlarının (2015) çalışmasında, birbirleriyle iş yapan firmalar (B2B) söz konusu olduğundan ve kurumsal itibarı ölçülmek istenen firmaların müşterileri

de firmalar olduğundan kurumsal itibarın boyutları önceki çalışmalardan farklı çıkmıştır. Dolayısıyla, bu çalışmalar kurumsal itibarın dinamik bir kavram olduğuna ve nitel ve nicel yöntemlerin birlikte kullanılmasıyla daha sağlıklı ölçümlere ulaşılabileceğine dair iyi birer örnek niteliği taşımaktadır. Bir diğer önemli husus ise, paydaşlar farklılaştığında kurumsal itibarın yapısının da değişmesidir. O halde, kurumsal itibarı ölçerken, ortak bir ölçeği tüm paydaşlara uygulamak yerine, her bir paydaş grubuyla ayrı ayrı yapılacak nitel araştırmaların daha sağlıklı sonuçlar verebileceğini öne sürmek mümkündür.

2.4.3. Kurumsal İtibar Ölçümlerine Yönelik Eleştiriler

Kurumsal itibarı ölçmeye dönük pek çok çalışma olsa da, bu çalışmalardan pek çoğu ciddi eleştirilere maruz kalmaktadır. Örneğin Wartick (2002: 390), kurumsal itibarı ölçmek için öncelikle kavramsal yapının oturması gerektiğini belirterek, itibarın kavramsal yapısı oturmadan ölçülmesinin sağlıklı olmayacağına değinmektedir. Hutton (2001: 249) ise, itibarın her paydaş için aynı olmadığına bu sebeple ölçümsel sıkıntılar olduğuna dikkat çekmiştir.

Özellikle sıralama bazlı ölçekler sıklıkla eleştirilmektedir. Fryxell ve Wang'a göre (1994: 11); Fortune 500'ün itibarı ölçmeye yönelik soruları ağırlıklı olarak finansal performansı ölçmekte, neredeyse bütün maddeler derecelendiricilerin firmanın finansal potansiyeline yönelik algılarından etkilenmektedir. Gerek ölçekte yer alan soruların niteliği gerekse bunların daha çok finansal performansı ölçmeye yönelik olmasıyla, bu ölçeğin itibarın finansal ve finansal olmayan boyutları arasındaki ayrımı göstermesinin pek mümkün olmadığını belirtmektedirler.

Buna ek olarak, Fortune'un finansal yapı ağırlıklı araştırması seçtiği derecelendiricilere de bağlı gibi görünmekte ve farklı gruplardan derecelendiricilerin seçilmesi durumunda sonuçların çok farklı olabilmesi muhtemel görünmektedir (Fryxell ve Wang, 1994: 13).

Fombrun (1998: 335-338) benzer eleştirilerde bulunarak, gazeteciler ve sosyal gözlemciler tarafından itibarı ölçmeye yönelik olarak geliştirilen ölçeklerin ciddi zafiyetler gösterdiğini belirtmiştir. Hem derecelendirdikleri şirketler hem de değerlendirici seçimleri sebebiyle sorunlu olduğunu, sistematik olarak belirlenmeyen ve genellikle belirli bir paydaş grubunun görüşlerini yansıtan dağınık kriterlere göre

değerlendirme yapıldığını ve genelleştirilmelerinin pek mümkün olmadığını belirtmektedir.

Fombrun ve arkadaşlarına (2000: 248) göre, mevcut itibar ölçümlerinde iki önemli sorunsal bulunmaktadır:

- Kurum liderleri ve finansal analistlerden oluşan dar katılımcı havuzları sebebiyle içerik geçerliliği zayıftır ve
- Ölçekler, kurumsal itibarı tam olarak ölçebilmek için gerekli olan tüm paydaşların algılarını yansıtabilecek maddeleri kapsamamaktadır.

Sarstedt ve arkadaşları (2013: 330-332) da mevcut itibar ölçeklerine yönelik eleştirilerde bulunmaktadır. Önceki eleştirilere ek olarak, Walsh ve Beatty'nin (2007) geliştirdiği müşteri tabanlı kurumsal itibar ölçeğinin yapısal geçerliliğini ve Schwaiger'in (2004) kurumsal itibar ölçeğinin içerik geçerliliğini sorgulamaktadır.

Sonuç olarak, kurumsal itibarı ölçmeye yönelik pek çok çalışmada mevcut ölçekler haklı gerekçelerle sıklıkla eleştirilmektedir. Bu da bir anlamda Wartick'in (2002) de uyardığı gibi kavramsal yapının tam olarak oturmamasından kaynaklanıyor gibi görünmektedir.

ÜÇÜNCÜ BÖLÜM
HACKTİVİZM VE KURUMSAL İTİBAR İLİŞKİSİNE YÖNELİK YAZINA BİR BAKIŞ VE KURAMSAL BİR MODEL ÖNERİSİ

3.1. HACKTİVİZM VE KURUMSAL İTİBAR İLİŞKİSİNE YÖNELİK YAZINA BİR BAKIŞ

Günümüz dünyasında, müşterilerin işlerini sanal ortamda yürüten firmalardan belirli beklentileri vardır. Müşteriler, ulaşmak istedikleri her anda firmaların çevrimiçi olmasını ve kişisel bilgilerini emanet ettiklerinde bunların korunmasını beklemektedirler. Dolayısıyla, bu beklentileri karşılamada başarısız olan firmalar müşteri kayıpları yaşayabilmektedirler. Buna ek olarak, herhangi bir haberin internet ve sosyal medya sayesinde hızla yayılması, sorunun kaynağı ne olursa olsun firmanın itibarına ciddi zararlar verebilmektedir. (Forbes, 2014: 12). İtibar nadir ve benzersiz olduğundan, farklılaşma ve rekabet avantajı kaynağı olarak görülmekte ve örgütlerin finansal değerini arttırdığından, firmalar bu soyut kaynağın zarar görmesini istememektedirler (King, 2008: 416).

Özellikle çevrimiçi satın alma deneyimlerinde, müşterinin kalite algısı, ürünün yanında ürünün alınmasıyla ilgili süreçlerin de değerlendirilmesiyle oluşmaktadır (Caruana ve Ewing, 2010: 1104). Bu süreçler büyük oranda işletmelerin yaptığı işleri destekleyen teknolojiden etkilenmektedir. Bu teknoloji çalışmadığında ise, sadece teknik ekibin problemi olmamakta, kurumsal itibar zedelenebilmekte ve sorun tepe yönetim düzeyinde bir soruna dönüşebilmektedir (Forbes, 2014: 2).

Pek çok müşteri hakkında pek fazla bir şey bilmedikleri çevrimiçi sitelerin ürünlerini almak konusunda isteksizdirler. Dolayısıyla, çevrimiçi perakendeciler için kurumsal itibar önemli bir varlık olarak görülmektedir (Caruana ve Ewing, 2010: 1104). Perakende sektörü gibi sektörlerde, müşteriler kurumun web sitesine giremediğinde sadece bir günlük satış kaybı yaşanmamakta, gelecekteki potansiyel satışlardan da mahrum kalma riski ortaya çıkmaktadır. Benzer şekilde, finansal kurumların yaşayacağı veri kayıpları müşterileri kaçırabilmektedir. İletişim ve bilişim firmalarında yaşanacak bir web sızıntısı ise, müşterilerin itibarlarını bu kurumlara emanet etme kararlarını sorgulamalarına neden olacaktır (Forbes, 2014: 4).

Sanal güvenlik herhangi bir firma için en ciddi risklerden biridir. Verileri ve sistemleri koruyacak bütün önlemler alınsa da sisteme girmek için tek bir açık yeterlidir. Firmaların sistemlerindeki tüm açıkları sürekli olarak savunmaları gerekirken, sanal saldırıyı gerçekleştirenlerin tek bir açığı bulmaları yeterlidir. Bu da, sanal saldırıyı gerçekleştirenleri her zaman avantajlı konuma getirmektedir (Forbes, 2014: 7).

Her ne kadar, geleneksel hack eylemlerinin aksine, kamu ve özel kuruluşlara yönelik hacktivist eylemler finansal kazanç sağlamak adına yapılmasa da, hedef alınan kurumların itibarlarını zedelemek için yapılmaktadır (Advisen, 2012: 2). Web site tahribatları ve yönlendirmeleri gibi nispeten daha az zararlı eylemler bir firmanın kamuoyu önünde küçük düşmesi gibi sonuçlar yaratsa da, geçici olduklarından kolaylıkla giderilebilmektedirler. Ancak, kurumsal verilerin sızdırılması ciddi problemlere yol açabilmektedir. Kuruma ait hassas bilgilerin ve işgörenlerin kişisel bilgilerinin sızdırılması kurumun itibarına ve inandırıcılığına zarar verecektir (Beach, 2012: 32).

Özellikle büyük miktarda hassas veriyi barındıran veya sanal güvenlik endüstrisinde lider olmakla övünen firmalar açısından, hacktivist saldırıların uzun vadede yıkıcı sonuçlara yol açabilme ihtimali bulunmaktadır (Beach, 2012: 36). Büyük çaplı hack eylemleri söz konusu olduğunda kurumsal itibar üzerindeki etkileri yıllar sürebilmektedir (Forbes, 2014: 3).

Yukarıdaki pek çok açıklamadan da görüldüğü üzere, hacktivist eylemlerin kurumsal itibar üzerinde önemli etkileri olabileceği söylenebilir. Ancak alan yazında aktivizm ve kurumsal itibar arasındaki ilişkilere dair pek çok çalışma olsa da (bkz. Coombs ve Holladay, 2012a; Coombs ve Holladay, 2012b; King, 2008; Waldron ve diğerleri, 2013; Van Cranenburgh ve diğerleri, 2013), hacktivizm ve kurumsal itibar ilişkisini inceleyen çalışma bulunmamaktadır. Bu çalışmanın, yazındaki bu eksikliği gidereceği düşünülmektedir.

Bu amaçla, PytlikZillig ve arkadaşlarının (2014) "Hacktivizme Destek ve Direnç Modeli" ve Schwaiger'in (2004) kurumsal itibar modeli bütünleştirici bir bakış açısıyla ele alınarak, hacktivizm ve kurumsal itibar ilişkisi üzerine bir model oluşturulmaya çalışılmıştır.

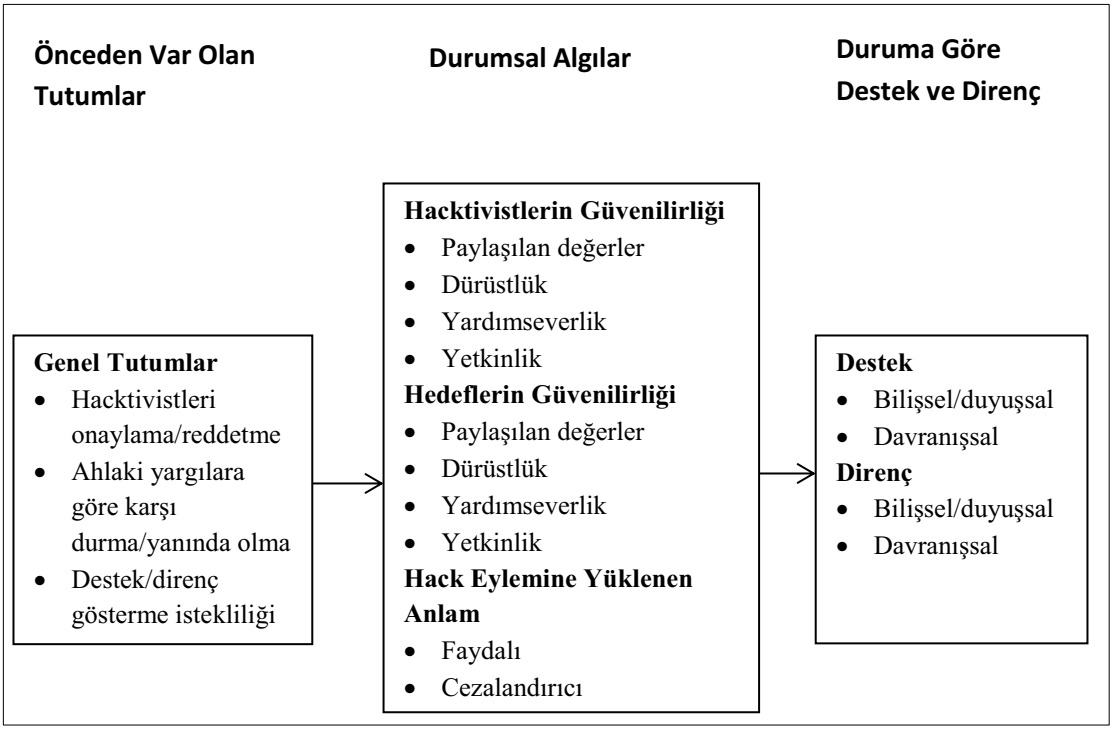
Hacktivist eylemlerin kurumsal itibar üzerinde yaratacağı etki paydaşların bu eylemleri nasıl algıladığına ve bu eylemlere destek verip vermeyeceğine göre değişecektir. Jordan ve Taylor'un (2004) da sıklıkla değindiği gibi, hacktivist eylemlerde kamunun desteğini almak eylemin etkinliğini arttırabilmektedir. O halde benzer bir etkinin, paydaşların bu eylemlere destek verip vermemesine göre oluşabileceğini söyleyebilmek mümkündür. Daha açık bir ifadeyle, paydaşların kurumsal itibar algılarının hacktivist eylemlerden etkilenme ihtimali ve eyleme yönelik desteğin tutumdan davranışa dönüşmesi durumunda bu etkinin derecesinin artma ihtimali bulunmaktadır. Örneğin; müşterilerin hacktivist eylemlerin haklı gerekçelerle yapıldığını düşünerek firmanın ürünlerini almayı bırakması, çalışanların ve sendikaların grev gibi aktivitelere girmesi gibi sonuçların ortaya çıkması olasıdır. Bu sonuçlara bağlı olarak, diğer paydaşların da hedefteki firmanın yetkinliğini sorgulaması ve firmaya yönelik sempatilerinin azalması gibi dolaylı etkilerin de ortaya çıkma ihtimali bulunmaktadır. Öte yandan, paydaşların desteğini almayan hacktivist eylemlerin kurumsal itibar üzerindeki etkisinin de farklı olması beklenebilir. Örneğin; yatırımcılar eylemin hedefindeki kurumun sorumluluklarını yerine getirdiğini, kurumun haksız gerekçelerle saldırıya uğradığını ve bu eylemlerin firmanın performansına önemli bir etkisi olmayacağını düşünerek firmadaki yatırımlarına devam edebilir. Dolayısıyla, paydaşların hacktivist eylemlere yönelik tutumsal ve davranışsal desteği veya direncinin hem kendi kurumsal itibar algılarını, hem de dolaylı yoldan diğer paydaşların kurumsal itibar algılarını nasıl etkilediğini ortaya koyabilmek önem arz etmektedir. Bu noktada, PytlikZillig ve arkadaşlarının (2014) "Hacktivizme Destek ve Direnç Modeli" paydaşların hacktivist eylemlere yönelik tutum ve davranışlarının anlaşılmasına yardımcı olacaktır.

3.2. HACKTİVİZM VE KURUMSAL İTİBAR İLİŞKİSİ YAZININA DAYALI KURAMSAL BİR MODEL ÖNERİSİ

PytlikZillig ve arkadaşları (2014), hacktivist eylemler söz konusu olduğunda bu eylemlerin izleyicileri konumunda olan bireylerin farklı senaryolarda hacktivizme olan destek veya dirençlerinin, izleyicilerin hacktivizme yönelik genel tutumları tarafından belirleneceğini, ancak bu ilişkide durumsal algıların aracı olduğunu belirtmektedir. PytlikZillig ve arkadaşlarının (2014: 3) araştırma modeli Şekil 3'te gösterilmektedir.

Bu modele göre, izleyicilerin hacktivizmle ilgili genel tutumları, izleyicilerin gerçekleştirilen hacktivist eylem özelindeki desteğinin veya direncinin belirleyicisi olacaktır. Genel tutumların ilk boyutu olan hacktivistleri onaylama/reddetme boyutu, izleyicilerin hacktivizme yönelik genel duyuşsal (hayranlık vb.) tepkilerini ifade etmektedir. İkinci boyutu olan ahlaki yargılara göre karşı/durma yanında olma boyutu, izleyicilerin hacktivizme yönelik genel bilişsel tepkilerini ifade etmekte ve son boyut olan destek/direnç gösterme istekliliği ise bu genel tepkilerin davranışsal yönünü ifade etmektedir.

Şekil 3: Hacktivizme Destek ve Direnç Modeli



Kaynak: PytlikZillig ve diğerleri, 2014: 3.

Durumsal algılarda ele alınan hacktivistlerin güvenilirliği ve hedeflerin güvenilirliği; Mayer ve diğerlerinin (1995) dürüstlük, yardımseverlik ve yetkinlik boyutları ve Siegrist ve diğerlerinin (2000) paylaşılan değerler boyutundan oluşturulan dört boyutlu yapılar olarak ele alınmaktadır. Mayer ve diğerlerine (1995: 719-720) göre dürüstlük; güvenilen tarafın güvenenin makul karşıladığı belirli ilkelere bağlı kalacağına dair güvenen tarafın algılarıyla ilgilidir. Yardımseverlik, güvenilen tarafın ne derece kendi çıkarına değil de güvenenin yararına olacak şekilde davranacağına dair güvenen tarafın inancıdır (Mayer ve diğerleri, 1995: 718).

Yetkinlik ise; bir tarafın belirli bir alanda etkili olmasını sağlayan beceri, yetkinlik ve özellikler grubudur. Bir tarafa yetkin olduğu alanlarda güven duyulabilirken, yetkin olmadığı alanlarda güven duyulmayacaktır (Mayer ve diğerleri, 1995: 717). Paylaşılan değerler; güvenilen tarafın belirli bir durumda öne çıkardığı değerleri (salient values), güvenen tarafın güvenilen tarafın bu değerleriyle ilgili bir sonuca vararak kendi değerleriyle olan benzerliğiyle kıyaslaması olarak ele alınmaktadır. Daha açık bir ifadeyle, bireyler belirli durumlarda belirli değerleri ön plana çıkarmakta ve bu bireylere yönelik güven oluşturacak taraf, kendi değerleri ve güvenilen tarafın bu belirli durumlarda ortaya çıkan değerleri arasındaki benzerliğe bakmaktadır. Güven ilişkisi tarafların değerlerinin benzeşmesine göre oluşmaktadır (Siegrist ve diğerleri, 2000: 355-356).

Durumsal algılarda ele alınan, hack eylemlerine yüklenen (atfedilen) anlam ise faydalı ve cezalandırıcı olmak üzere iki boyutta ele alınmaktadır. Hareli ve Weiner (2002) amaçların ve sonuçların ve bunların yorumlanmasının sosyal olarak belirlendiğini ve bireylerin güdülerinin, duygularının ve davranışlarının etraflarındaki dünyayı yorumlama biçimlerine göre atfettikleri anlamlar doğrultusunda şekillendiğini öne sürmektedir. Buradan yola çıkan PytlikZillig ve arkadaşları (2014: 5), Gandhi ve arkadaşlarının (2011: 36) sanal saldırı güdüleri olarak ele aldığı tüm güdülere faydalı (sanal casusluk vb.) ve cezalandırıcı (misilleme vb.) olmak üzere iki ana anlam atfedilebileceğini öne sürmektedir. Ancak burada dikkat edilmesi gereken nokta, faydalı boyutunun hacktivistlerin topluma hizmet edecek şekilde davranması olarak ele alınmasıdır. Cezalandırıcı boyutu ise, hedefin gerçekleştirilen eylemi hak edip etmediğiyle ilgili özellikleri temsil etmektedir.

Modelde ele alınan, duruma göre izleyicilerin göstereceği destek/direnç ise tutumsal (bilişsel ve duyuşsal) ve davranışsal olmak üzere iki ana boyutta ele alınmakta ve izleyicilerin hacktivist eylemlere vereceği tutumsal ve davranışsal tepkileri ifade etmektedir.

Bu modelden hareketle, ticari bir işletmeye yönelik hacktivist eylemler söz konusu olduğunda, izleyicilerin kurumun paydaşları olarak ele alınabileceği öne sürülebilmektedir. Hacktivist eylemlere destek verme veya direnç göstermeye

yönelik tutumların ise, paydaş penceresinden bakılarak hacktivist eylemlere yönelik olumlu tutum veya olumsuz tutum olarak ele alınması yerinde olacaktır.

Kurumun paydaşlarının hacktivizme yönelik genel tutumlarının, gerçekleştirilen hacktivist eyleme yönelik tutum ve davranışlarını doğrudan etkileyip etkilemediğine değinmek gerekmektedir. Planlı davranış kuramına göre; bireylerin genel tutumları ve kişilik özellikleri gibi bireysel faktörler, eğitim ve kültür gibi sosyal faktörler ve medya gibi bilgisel faktörler bireylerin inanışlarını şekillendirmekte ve bu da bireylerin belirli davranışları gerçekleştirmeleri yönündeki niyetlerini belirlemektedir (Ajzen ve Fishbein, 2005: 193-194). Örneğin, bazı araştırmacılar (Gray ve Balmer, 1998; Deephouse, 2000) medyanın kurumsal itibarın oluşmasındaki etkisine değinmektedir. Ayrıca, hacktivist bir eylemin doğrudan etki derecesinin düşük olması durumunda bile, medyada geniş şekilde yer bulduğu takdirde hedefteki kurumun kamu önünde küçük düşme derecesini arttıracağı söylenebilmektedir (Beach, 2012: 36). Buna ek olarak internet çağında ele alınması gereken medya, sosyal medyanın da içinde bulunduğu çok daha geniş bir mecradır. Çevrimiçi forumlar gibi sosyal medya kanallarında bu eylemlerin tartışılması, belirli bir süre içinde paydaşların tutum ve davranışlarını da etkileyebilecektir. Nitekim Park ve Lee (2007: 348) çevrimiçi forumlarda tek bir olumsuz yorumun bile kurumsal itibar algısı üzerinde önemli bir etkisinin olabileceğine değinmektedir.

Bu çerçevede, paydaşların hacktivistlere yönelik genel tutumlarının olumlu olması, onların hacktivist eylemlere yönelik tutumlarının da olumlu olma ihtimalini güçlendirecek, genel tutumlarının olumsuz olması durumunda ise hacktivist eylemlere yönelik tutumları da olumsuz olacaktır. Nitekim PytlikZillig ve arkadaşları (2014: 10) özellikle hayranlığın hacktivist eyleme yönelik desteği belirlediğini ve hacktivist eylemi bildirme istekliliğinin ise direnci belirlediği sonucuna ulaşmıştır. Ancak ahlaki yargıların bu ilişkide bir etkisi gözlenmemiştir. Yine de, paydaşların farklı bir örneklem grubunu temsil etme olasılığı ve ticari işletmelere yönelik eylemlerin de farklı durumları temsil etme olasılıkları göz önünde bulundurulduğunda, ahlaki yargıların bu ilişkiyi etkileme olasılığı bulunmaktadır.

Hacktivizm ve kurumsal itibar ilişkisi söz konusu olduğunda paydaşların ticari işletmelere yönelik genel tutumlarının da etkili olabileceği dikkate alınmalıdır.

Macleod'a (1967: 67-68) göre; bir firmanın itibarının gelişmesine veya kısıtlanmasına neden olan 3 önemli etmen vardır. Bunlar kamunun;

1) büyük ölçekli işletmelere yönelik genel algıları,

2) şirketin içinde bulunduğu endüstriye yönelik algıları ve

3) rakipleriyle kıyaslandığında bir şirketin itibarının nasıl algılandığıdır.

Buradan yola çıkarak, paydaşların kurumsal itibar algısında hacktivist eylemin hedefindeki kurumun içinde bulunduğu endüstriye yönelik genel tutumlarının ve büyük ölçekli işletmelere yönelik genel tutumlarının da etkili olabileceğini öne sürebilmek mümkündür. Ancak, durumsal faktörlerde ele alındığı gibi özellikle paylaşılan değerler bağlamında bakıldığında, hacktivistlerin görüşleriyle benzer görüşleri paylaşan paydaşların, hacktivist eylemi gerçekleştirene güven duyarak hack eylemine olumlu bakabilme ihtimali vardır. Örneğin, özellikle kitlesel eylem hacktivizmi gibi hacktivizm türlerinde, büyük ölçekli işletmelere yönelik olumsuz bir bakış açısı bulunmaktadır. Dolayısıyla büyük ölçekli işletmelere yönelik olumsuz tutumlara sahip paydaşların, hack eylemini gerçekleştiren grubun kitlesel eylem hacktivizmini yansıtması durumunda, eylemi gerçekleştiren paydaşa yönelik güveninin derecesinin yükselme olasılığı bulunmaktadır. Bu çerçevede paydaşların, gerek büyük ölçekli işletmelere yönelik genel tutumları, gerekse hedefteki kurumun içinde bulunduğu endüstriye yönelik genel tutumları, hacktivizm ve kurumsal itibar ilişkisinde, hacktivistlere yönelik genel tutumların da içinde yer aldığı önceden var olan tutumlar grubuna dahil edilmelidir. Bu açıklamalar ışığında, aşağıdaki önermeyi geliştirebilmek mümkündür.

Önerme 1: Paydaşların hacktivistlere yönelik genel tutumları ile hacktivist eyleme yönelik olumlu veya olumsuz tutumları arasında doğrudan anlamlı bir ilişki vardır.

PytlikZillig ve arkadaşları (2014: 4-5), izleyicilerin hacktivist eylemi gerçekleştirenlere ve eylemin hedefindeki kuruma duydukları güvenin, eyleme destek veya direnç göstermelerinin belirleyicisi olduğunu öne sürmektedir. Nitekim yaşanmış örnekler bu görüşü destekler niteliktedir. 2012 yılında Norton Antivirüs programının üreticisi Symantec'e yönelik olarak gerçekleştirilen hack eylemi buna verilebilecek güzel bir örnektir.

10 Ocak 2012 yılında James Gross isimli bir Amerikan vatandaşı, tam sürümün satın alınması için Norton antivirüs programının kullanıcılara sahte virüs uyarıları verdiğini iddia ederek Symantec'e dava açmıştır. Bunun üzerine Anonymous ile ilişkilendirilen Lords of Dharmaraja adlı grubun bir üyesi Norton antivirüs programının kaynak kodlarını yayınlayacağını ilan etmiştir. Symantec önce kaynak kodlarının üçüncü bir taraftan çalındığını iddia etmiş, sonradan ise 2006 yılında sistemlerine sızıldığını ve verilerin çalındığını itiraf etmiştir. Bu hacktivist girişim Symantec açısından oldukça küçük düşürücü olmuş ve firmanın güvenlik zafiyetlerini gözler önüne sermiştir (Beach, 2012: 44-45).

Bu örnekten de görüleceği üzere, özellikle Symantec'in paydaşlarını doğru şekilde bilgilendirmemesinin, kuruma duyulan güveni önemli ölçüde zedelemiş olma ihtimali vardır. Böyle bir durumda, paydaşların hacktivist eyleme yönelik olumlu veya olumsuz tutumlarının kuruma duyulan güvenle ilişkili olabileceğini söyleyebilmek mümkündür. Öte yandan, bu ilişki paydaşların hacktivist eylemi gerçekleştiren kişiye olan güvenine göre de değişebilecektir. Çünkü her ne kadar paydaşların kuruma olan güvenleri sarsılmış olabilse de, eylemi gerçekleştiren tarafın paydaşların çıkarlarına hizmet etmediği düşüncesiyle bir güvensizlik oluşabilme ihtimali vardır. PytlikZillig ve diğerlerinin (2014) model açıklamasında da belirtildiği üzere güven; tarafların dürüstlüğü, yardımseverlikleri, yetkinlikleri ve paydaşların taraflarla paylaştıkları değerlere yönelik algılarından oluşmaktadır. Bu çerçevede, Symantec'in güvenilirliğinin sorgulanması hiç şaşırtıcı olmayacaktır. Benzer şekilde, eylemi gerçekleştiren kişinin her ne kadar yetkin olabileceğine dair bir algı oluşabilse de, gerçekleştirdiği eylemle paydaşlara yardım edip etmediği tartışmaya açıktır. Dolayısıyla, paydaşların eyleme yönelik tutumlarının, taraflara duyduğu güvenden etkilenebileceğini söyleyebilmek mümkündür. Nitekim PytlikZillig ve arkadaşları (2014: 10) hem hedefin hem de hacktivist eylemi gerçekleştirenlerin güvenilirliğinin, izleyicinin eyleme yönelik destek veya direncini belirlediği sonucuna ulaşmışlardır. Burada dikkati çeken bir diğer nokta, tüm senaryolarda hacktivistlere duyulan güvenin hedefe duyulan güvene kıyasla izleyicilerin tutumlarını daha çok etkilediğinin görülmesidir. Bu açıklamalar ışığında, aşağıdaki önermeleri geliştirebilmek mümkündür:

Önerme 2: Paydaşların, hacktivist eylemi gerçekleştirenlere duydukları güven ile hacktivist eyleme yönelik olumlu veya olumsuz tutumları arasında anlamlı bir ilişki vardır.

Önerme 3: Paydaşların, hacktivist eylemin hedefindeki kuruma duydukları güven ile hacktivist eyleme yönelik olumlu veya olumsuz tutumları arasında anlamlı bir ilişki vardır.

Ayrıca PytlikZillig ve arkadaşları (2014: 12), modelde öne sürdükleri aracılık etkisini de doğrulamıştır. Buradan hareketle aşağıdaki önermeleri geliştirebilmek mümkündür:

Önerme 4: Paydaşların, hacktivistlere yönelik genel tutumları ile hacktivist eyleme yönelik olumlu veya olumsuz tutumları arasındaki ilişkide hacktivist eylemi gerçekleştirenlere duydukları güvenin aracılık rolü vardır.

Önerme 5: Paydaşların, hacktivistlere yönelik genel tutumları ile hacktivist eyleme yönelik olumlu veya olumsuz tutumları arasındaki ilişkide hacktivist eylemin hedefindeki kuruma duydukları güvenin aracılık rolü vardır.

Diğer taraftan, Şekil 3'teki modelde değinildiği üzere, bireylerin eyleme yükledikleri anlamlar da tutumların oluşmasında etkili olabilmektedir. Örneğin; paydaşların kurumun bu eylemin hedefinde olmasının geçerli bir nedeni olup olmadığını sorgulaması muhtemeldir. Benzer şekilde, eylemi gerçekleştirenlerin gerekçelerini paydaşların nasıl yorumlayacağı da önemli olabilmektedir. 2011'de Stratfor'un hacktivistler tarafından hedef alınmasına yönelik örnek, anlatılmak istenen hususun daha iyi anlaşılması açısından yararlı olacaktır.

Bir danışmanlık firması olan Stratfor, Aralık 2011'de Antisec adlı bir oluşum tarafından hacklenerek, müşterilerinin kişisel bilgileri ve kredi kartı bilgileri internette yayınlanmıştır. Bu eylemin temel gerekçesi ise Stratfor'un oldukça büyük bir müşteri havuzu olmasına rağmen güvenliğinin ne derece zayıf olduğunu göstermektir. Sektöründe güvenilir bir firma itibarına sahip olan Stratfor açısından bu eylem ciddi zarara sebep olmuştur. Kurumun tahmin ettiği ekonomik kayıp 2 milyon dolardan fazladır. Stratfor eylemi, hacktivistlerin sadece güvenlik zafiyetlerini göstermek için bir kuruma saldırabileceğini göstermesi açısından önemli bir örnek teşkil etmektedir (Beach, 2012: 51-52).

Yukarıdaki örnek göz önünde bulundurulduğunda paydaşların eyleme atfedecekleri anlam farklılaşabilecektir. Örneğin, kimlik bilgileri çalınan müşterilerin eylemi kamuya faydalı bir eylem olarak yorumlamaları pek mümkün gözükmemektedir. Dolayısıyla, bu müşterilerin hacktivist eyleme yönelik olumlu tutum geliştirme olasılıklarının düşük olduğunu söyleyebilmek mümkündür. Bunun yanında, kurumun güvenlik zafiyetlerine sahip olduğunu görmeleri, kurumun cezalandırılmasını doğru bulmaları yönünde bir görüşleri oluşmasına da sebep olabilir. Yine de bu görüşün hacktivist eyleme yönelik olumlu bir tutum geliştirme sonucuna yol açmasının zor olduğu düşünülmektedir. Nitekim, PytlikZillig ve diğerlerinin (2014) eyleme atfedilen anlama ilişkin elde ettiği bulgular bu görüşü destekler niteliktedir. PytlikZillig ve arkadaşları (2014, 5), önceki araştırmalardan (Feshbach, 1970; Kanekar ve diğerleri, 1981) yola çıkarak, insanların cezalandırıcı güdülerle gerçekleştirilen eylemleri, faydalı/araçsal güdülerle gerçekleştirilen eylemlere kıyasla daha düşmancıl ve ahlaki açıdan daha zayıf olarak algıladıklarına değinmektedir. Bu çerçevede, cezalandırıcı eylemlerin hacktivizme yönelik desteği olumsuz, direnci ise olumlu etkileyeceğini, faydalı eylemler içinse tam tersi bir durumun söz konusu olacağını öne sürmektedir. Ancak, araştırma sonuçları sadece faydalı eylemler için öne sürülen önermelerin desteklendiğini göstermektedir. O halde, eylemlere atfedilen anlamlar ve izleyicilerin gerçekleştirilen eyleme yönelik tutumları arasındaki ilişkinin dinamik olduğu ve eylem özelinde çok farklı sonuçlar verebileceğini öne sürebilmek mümkündür. Tüm bu açıklamalar doğrultusunda aşağıdaki önerme sunulmaktadır:

Önerme 6: Paydaşların hack eylemine yüklediği anlam ile paydaşların hack eylemine yönelik olumlu veya olumsuz tutumları arasında anlamlı bir ilişki vardır.

Ayrıca, PytlikZillig ve arkadaşları (2014: 12) atfedilen anlamların bir senaryo dışında hepsinde aracılık etkisi olduğunu doğrulamışlardır. O halde aşağıdaki önermeyi sunabilmek mümkündür:

Önerme 7: Paydaşların, hacktivistlere yönelik genel tutumları ile hacktivist eyleme yönelik olumlu veya olumsuz tutumları arasındaki ilişkide hack eylemine yükledikleri anlamın aracılık rolü vardır.

Yukarıdaki önermeler ışığında, paydaşların hacktivist eylemlere yönelik olumlu veya olumsuz tutumlarının belirleyicileri açıklanmaya çalışılmıştır. Buna

karşın, paydaşların hacktivist eylemlere yönelik tutumlarının kurumsal itibarla nasıl bir ilişkisi olduğuna yönelik bağlantılar henüz kurulmamıştır. O halde bu eksikliği gidermek adına, araştırma modelinin ikinci parçasını oluşturan Schwaiger'in (2004) kurumsal itibar modeline değinmek ve hacktivizmle kurumsal itibar ilişkisine yönelik bağlantıları kurmak gerekecektir.

Schwaiger'i (2004: 49) takiben bu çalışmada kurumsal itibar, "tutumun; öznel, duyuşsal ve bilişsel zihniyetleri ifade ettiği tutumsal bir yapı" olarak ele alınmaktadır. Bu yapı Schwaiger'in (2004: 49) de belirttiği üzere, hem kurumsal özelliklerle ilgili öznel algıları temsil etmesi bakımından, hem de bireyin kuruma yönelik içsel eğilimlerini yansıtmasıyla kapsayıcı bir yapı gibi görünmektedir.

Schwaiger (2004) kurumsal itibarı; yetkinlik ve sempatiden oluşan iki boyutlu bir yapı olarak ele almaktadır. Yetkinlik, kurumsal itibarın bilişsel yönünü temsil ederken, sempati duyuşsal yönünü temsil etmektedir. Bu iki boyutun ise; kalite, performans, sorumluluk ve cazibe (çekicilik) olmak üzere dört temel göstergesi bulunmaktadır. Schwaiger'e (2004: 62-63) göre kalite, firmanın ürün hizmet kalitesi ve müşteri yönelimi gibi özelliklerini temsil etmektedir. Performans, firmanın finansal performansı ve yatırım potansiyeli gibi özelliklerini temsil etmektedir. Sorumluluk, firmanın topluma ve çevreye karşı sorumlu bir vatandaş olmasıyla ilgili özelliklerini temsil etmektedir. Cazibe (çekicilik) ise, firmanın yetenekli adayları işe almada başarılı olması ve çalışılmak istenen bir yer olması gibi özelliklerini temsil etmektedir.

Kurumsal itibarın göstergeleri ve boyutları arasında önemli bağlantılar bulunmakla birlikte bu bağlantılara geçmeden önce, paydaşlarda hacktivist eylemlere yönelik ortaya çıkan olumlu veya olumsuz tutumlarının kurumsal itibara yönelik tutumlarını nasıl etkileyebileceğine değinmek gerekmektedir. Yine planlı davranış kuramından hareketle, yukarıda ele alınan süreçler sonucunda paydaşın hacktivist eyleme yönelik oluşturduğu tutumlar, kurumsal itibarla ilgili tutumlarının öncülü olabilecek hali hazırda var olan bir tutumdur. Dolayısıyla, genel tutumların hacktivist eyleme yönelik tutumların belirleyicisi olduğu gibi, hacktivist eylemi destekleme veya direnç göstermeye yönelik olarak paydaşlarda gelişen tutumun, kurumsal itibara yönelik tutumlarını doğrudan etkileyebileceği öngörülmektedir. Bu bağlamda aşağıdaki önermeleri sunabilmek mümkündür:

Önerme 8: Paydaşların hacktivist eyleme yönelik olumlu/olumsuz tutumları ile kurumsal itibarın yetkinlik boyutu arasında anlamlı bir ilişki vardır.

Önerme 9: Paydaşların hacktivist eyleme yönelik olumlu/olumsuz tutumları ile kurumsal itibarın sempati boyutu arasında anlamlı bir ilişki vardır.

Ajzen ve Fishbein'e (2005: 185) göre, genel tutumlar algıları da etkilemektedir. Bir nesne hakkında olumlu tutum geliştiren bireylerin, bu nesnenin önce olumlu özelliklerine dikkat etme olasılıkları vardır. Bir nesne hakkında olumsuz tutum geliştiren bireylerin ise, bu nesnenin olumsuz özelliklerini daha önce fark etmesi muhtemeldir. Dolayısıyla, nesneye yönelik bu algılar (sosyal normlar gibi bağlamsal faktörlerle birlikte), bireyin olayı tanımlamasını etkileyecek ve nesneyi olumlu veya olumsuz değerlendirmesine göre davranışlarına yön verecektir. Buradan hareketle, paydaşların hack eylemine yönelik olumlu veya olumsuz tutum geliştirmelerinin; firmanın kalitesine, performansına, sorumluluğuna ve cazibesine yönelik algılarını da etkileyeceği öne sürülebilmektedir.

Bu bağlamda, hack eylemine yönelik olumlu tutum geliştiren paydaşların, firmanın ürün hizmet kalitesi ve müşteri yönelimi gibi kalite özellikleri söz konusu olduğunda, önce bu özelliklerle ilgili eksikliklere dikkat etmesi ve firmanın kalitesini olumsuz algılaması muhtemel görünmektedir. Paydaşların hack eylemine yönelik olumsuz tutum geliştirmeleri durumunda ise, firmanın kalitesine yönelik algılarının olumlu olması beklenmektedir. O halde, aşağıdaki önermeleri ortaya atabilmek mümkündür:

Önerme 10: Paydaşların hacktivist eyleme yönelik olumlu/olumsuz tutumları ile kurumun kalitesine yönelik algıları arasında anlamlı bir ilişki vardır.

Benzer etkilerin diğer kurumsal itibar göstergeleri üzerinde de görülme olasılığı bulunmaktadır. Paydaşların, hacktivist eyleme yönelik tutumları olumlu olduğunda; firmanın performansı, sorumluluğu ve cazibesiyle ilgili sorunların daha çok dikkatini çekmesi ve dolayısıyla algılarının olumsuz olarak şekillenmesi olası görünmektedir. Bu durumda aşağıdaki önermeleri öne sürebilmek mümkündür:

Önerme 11: Paydaşların hacktivist eyleme yönelik olumlu/olumsuz tutumları ile kurumun performansına yönelik algıları arasında anlamlı bir ilişki vardır.

Önerme 12: Paydaşların hacktivist eyleme yönelik olumlu/olumsuz tutumları ile kurumun sorumluluğuna yönelik algıları arasında anlamlı bir ilişki vardır.

Önerme 13: Paydaşların hacktivist eyleme yönelik olumlu/olumsuz tutumları ile kurumun cazibesine yönelik algıları arasında anlamlı bir ilişki vardır.

Kurumsal itibarın göstergeleri ve kurumsal itibarın boyutları arasında da bazı ilişkilerin varlığından söz edebilmek mümkündür. Bu göstergeler, kurumsal itibar bölümünde ayrıntılı olarak ele alındığından burada sadece teorik bağları kurabilmek adına yapılan araştırmalara kısaca değinilecektir.

Pek çok araştırmacı (Ely ve Valimaki, 2003; Yoo, Donthu ve Lee, 2000; Dollinger, Golden ve Saxton, 1997; Preston ve O'Bannon, 1997; Turban ve Greening, 1997) algılanan kaliteyi kurumsal itibarın önemli bir göstergesi olarak görmektedir (Rhee ve Valdez, 2009: 149-150). Schwaiger'e (2004: 65-66) göre paydaşların kurumun kalitesine yönelik algıları, kurumsal itibarın hem sempati hem de yetkinlik boyutlarını olumlu etkilemektedir. Daha açık bir ifadeyle, paydaşlar kurumun müşterileriyle iyi ilişkiler kurduğunu ve kaliteli ürün ve hizmetler sunduğunu düşünüyorsa, firmanın yaptığı işte iyi olduğunu düşünmekte ve firmaya sempati duymaktadırlar. Bu bilgilerden hareketle, aşağıdaki önermeler sunulabilmektedir:

Önerme 14: Paydaşların kurumun kalitesine yönelik algıları ile kurumsal itibarın yetkinlik boyutu arasında pozitif anlamlı bir ilişki vardır.

Önerme 15: Paydaşların kurumun kalitesine yönelik algıları ile kurumsal itibarın sempati boyutu arasında pozitif anlamlı bir ilişki vardır.

Firma performansı ve kurumsal itibar ilişkisi üzerine yapılan pek çok araştırmada (Healy ve Palepu, 1993; Toms, 2002; McGuire, Sundgren ve Schneeweis, 1988; Dollinger, Golden ve Saxton, 1997; Preston ve O'Bannon, 1997; Clark ve Montgomery, 1998; Cable ve Graham, 2000; Staw ve Epstein, 2000), finansal performansın kurumsal itibarın öncüsü olduğu öne sürülmektedir (Rhee ve Valdez, 2009: 149-150). Schwaiger'e (2004: 65-66) göre, paydaşların kurumun performansına yönelik algıları, kurumsal itibarın yetkinlik boyutunu olumlu etkilemekte ancak sempati boyutunu olumsuz etkilemektedir. Buradan yola çıkarak, aşağıdaki önermeleri ortaya atabilmek mümkündür.

Önerme 16: Paydaşların kurumun performansına yönelik algıları ile kurumsal itibarın yetkinlik boyutu arasında pozitif anlamlı bir ilişki vardır.

Önerme 17: Paydaşların kurumun performansına yönelik algıları ile kurumsal itibarın sempati boyutu arasında negatif anlamlı bir ilişki vardır.

Firmanın sosyal ve çevresel sorumluluklarını yerine getirmesi (McGuire, Sundgren ve Schneeweis, 1988; Preston ve O'Bannon, 1997; Turban ve Greening, 1997) kurumsal itibarın bir diğer önemli göstergesi olarak görülmektedir. Schwaiger'e (2004: 65-66) göre, paydaşların kurumun sosyal ve çevresel sorumluklarını yerine getirdiğine yönelik algıları, kurumsal itibarın sempati boyutunu olumlu etkilemekte ancak yetkinlik boyutunu olumsuz etkilemektedir. Bu bilgiler ışığında aşağıdaki önermeleri sunmak mümkündür:

Önerme 18: Paydaşların kurumun sorumluluğuna yönelik algıları ile kurumsal itibarın yetkinlik boyutu arasında negatif anlamlı bir ilişki vardır.

Önerme 19: Paydaşların kurumun sorumluluğuna yönelik algıları ile kurumsal itibarın sempati boyutu arasında pozitif anlamlı bir ilişki vardır.

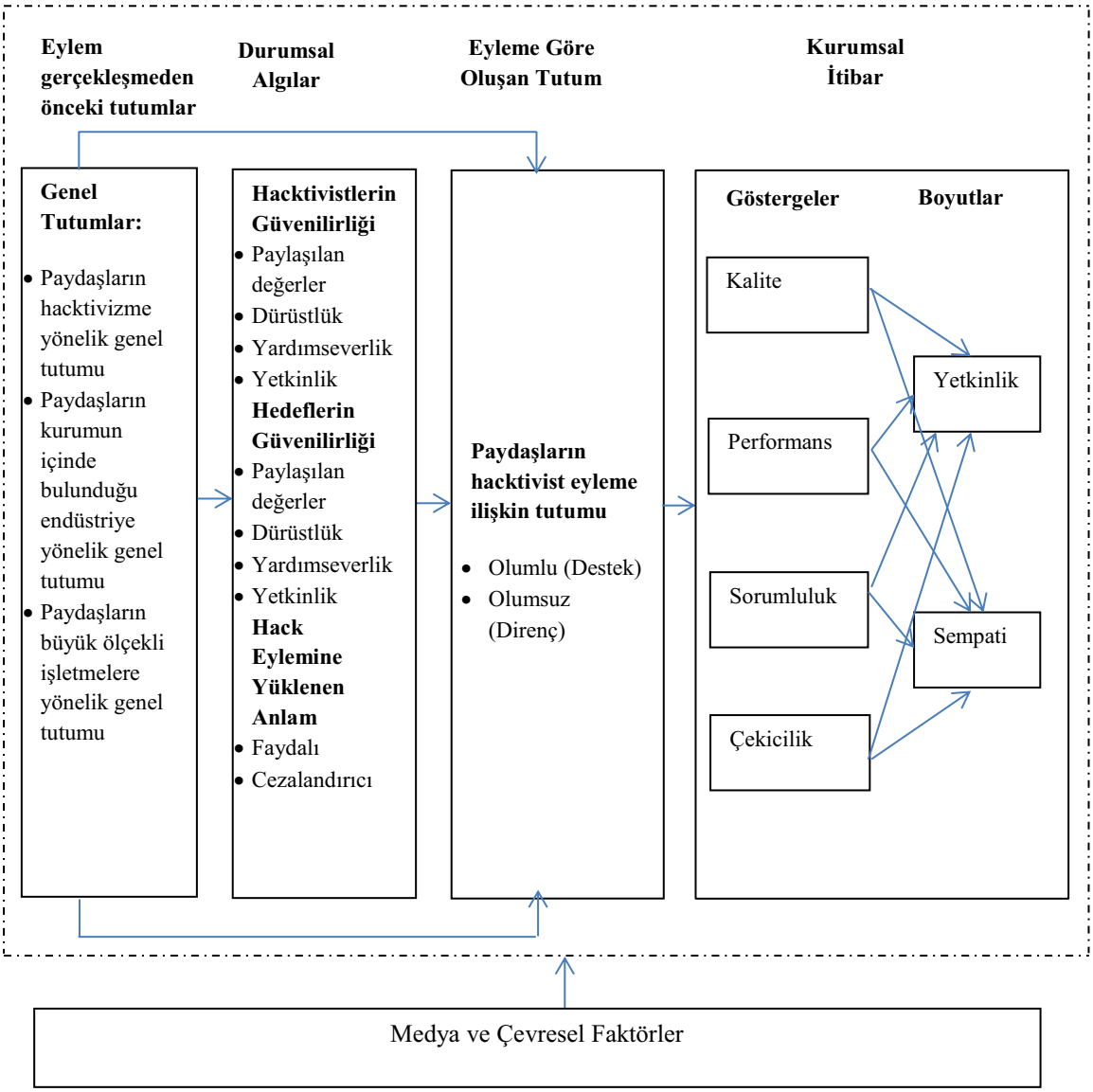
Son olarak ise, firmanın cazibesi ve kurumsal itibar boyutlarıyla ilişkisine kısaca değinmekte yarar vardır. Firmanın çekiciliği veya cazibesi de önemli bir kurumsal itibar göstergesi olarak görülmektedir. Schwaiger'e (2004: 65-66) göre, paydaşların kurumun cazibesine yönelik algıları, kurumsal itibarın hem sempati hem de yetkinlik boyutlarını olumlu etkilemektedir. O halde, aşağıdaki önermeleri sunabilmek mümkündür:

Önerme 20: Paydaşların kurumun cazibesine yönelik algıları ile kurumsal itibarın yetkinlik boyutu arasında pozitif anlamlı bir ilişki vardır.

Önerme 21: Paydaşların kurumun cazibesine yönelik algıları ile kurumsal itibarın sempati boyutu arasında pozitif anlamlı bir ilişki vardır.

Yukarıda ele alınan önermeler doğrultusunda tasarımlanan araştırma modeli Şekil 4'te gösterilmektedir.

Şekil 4: Hacktivizm ve Kurumsal İtibar İlişkisi Üzerine Geliştirilen Model



SONUÇ

Günümüzde bilgi teknolojileri firmalara önemli avantajlar sunmakta, ancak; özellikle internetin doğası gereği sistem sızıntılarına izin veren yapısı, aynı zamanda firmalar için ciddi riskleri de beraberinde getirmektedir. Firmaların bilgi teknolojilerine bu derece bağımlı olduğu bir zamanda, bu teknolojilerin geçici olarak devre dışı kalması, önemli problemlere yol açabilmektedir. Bu teknolojilerin geçici veya kalıcı olarak devre dışı kalması, firmaların yaşayacağı finansal kayıpların yanında, paydaşlarının firmayla ilgili algılarını da etkileyebilmektedir.

Özellikle son yıllarda hack eylemleri, firmalar için ciddi bir risk oluşturmaya başlamıştır. Bu eylemlerin çoğu kişisel çıkar sağlamak adına yapılsa da, hacktivist oluşumların gerçekleştirdiği eylemler genellikle firmaların faaliyetlerine bir tepki olarak ortaya çıkmaktadır. Bu bağlamda, firmaların paydaşlarının hacktivist eylemleri nasıl algıladığı, firmaların itibarına yönelik algılarını şekillendirebilmektedir.

Kurumsal itibar çalışma boyunca da sıklıkla ele alındığı gibi; firmaların performanslarıyla, topluma ve çevreye karşı gösterdikleri hassasiyetle, ürün ve hizmetlerinin kalitesinin yanında müşterileriyle olan iyi ilişkileriyle ve çalışanları için iyi bir işveren olmakla birlikte, potansiyel adayları firmaya çekebilme kabiliyetiyle de yakından ilişkili görülmektedir. Pek çok araştırmacı, firmaların bu özelliklerini iyi bir kurumsal itibarı oluşturan temel unsurlar olarak ele almaktadır. Paydaşların, bu unsurlardan biri veya bir kaçına yönelik olumsuz tutum geliştirmeleri ise, onların kurumsal itibar algılarını etkileyebilmekte ve kurumsal itibarı zedelenen firmalar maddi kayıpların yanında, toplum nezdinde meşruiyetlerini de yitirebilmektedirler.

Hacktivistler, firmalara çeşitli sebeplerle saldırabilmektedir. Bu sebeplerin en başında ise, firmaların topluma ilişkin sorumluluklarını yerine getirememesi veya toplumun faydasına çalışmadığına dair düşünceleridir. Nitekim, Fombrun (2005: 7), toplumun firmaların belirli sosyal ve etik kriterlere uyması yönündeki beklentilerinin arttığına ve bunun firmaların itibarını önemli ölçüde etkileyebileceğine değinmektedir. Benzer şekilde Gray ve Balmer (1998: 699) da, toplumsal eylem gruplarının kurumlara yönelik eleştiri ve eylemlerinin ekonomik olarak etkili olsun veya olmasın, bazı müşterilere yansıyarak kurumların kamudaki itibarını

etkileyebileceğine değinmektedir. Bu kapsamda, hacktivistlerin toplumsal bir fayda sağlamak amacıyla eylemler gerçekleştirdiğini düşünen paydaşların, bu eylemlerin hedefindeki kurumlara yönelik itibar algılarının önemli ölçüde zedelenebileceğini öne sürebilmek mümkündür.

Hacktivistler, zaman zaman firmalara ait hassas bilgileri de kamuoyuna sunmaktadır. Lange ve arkadaşlarının (2011: 154) ifade ettiği gibi, itibarın kökeni firmanın geçmişteki davranışlarına dayansa da, geçmişe dair yeni bilgiler açığa çıktığında veya örgütün son zamanlardaki davranışları gözlemcileri rahatsız edici olduğunda büyük oranda değişebilmektedir. O halde, hacktivistlerin kamuoyuyla paylaştığı bilgilerin, paydaşların hedefteki kurumu yeniden değerlendirmesine yol açacağını söyleyebilmek mümkündür.

Bunlara ek olarak, hacktivist eylemlerin özellikle çevrimiçi satış yapan firmalara ciddi ölçüde zarar verebilme potansiyeli bulunmaktadır. Web siteleri geçici olarak devre dışı kalan firmalar, yaşayacakları finansal kayıpların yanında müşterilerini kaybetme tehlikesiyle de karşı karşıya kalabilmektedir. Ayrıca firmaların güvenlik zafiyetlerini göstermesi bakımından yetkinliklerinin sorgulanmasına da yol açabilmektedir. Dolayısıyla, yaşanan bu doğrudan kayıpların paydaşların kurumsal itibara yönelik algılarını etkileyebilme olasılığı da göz ardı edilmemelidir.

Hacktivist eylemler, sembolik eylemlerden firmalara ait hassas bilgilerin ele geçirilerek kamuoyuyla paylaşılmasına kadar pek çok farklı şekillerde ortaya çıkabilmektedirler. Bu kapsamda, hacktivist eylemlerin paydaşların kurumsal itibar algıları üzerinde yaratabileceği muhtemel etkilerin şiddetinin de bu eylemlerin türüne göre değişebileceği öngörülebilmektedir. Örneğin; bir firmanın müşterilerinin kredi kartı bilgilerinin çalınarak internette paylaşılması veya bu müşterilerin hesaplarından çeşitli toplumsal yardım örgütlerine paralar aktarılmasının yaratacağı etkiyle, bu firmanın web sitesinin içeriği değiştirilerek "Yunus Katliamına Dur Deyin" şeklinde bir mesajın yerleştirmesi gibi sembolik bir eylemin yaratacağı etkinin aynı olmayacağı açıktır. Paydaşların büyük çoğunluğunun bu sembolik eylemi önemsiz olarak göreceği ortadadır. Ancak, ilk senaryoda olduğu gibi müşterilerinin kredi kartı bilgilerini çaldıran firmaların kurumsal itibarlarının böyle bir olaydan etkilenmeme olasılığı yok denecek kadar azdır. O halde, bir firmanın hacktivist eylemlere maruz

kalması durumunda, paydaşlarının kurumsal itibar algılarının farklı eylemlere göre farklı şekillerde etkilenebileceğini öne sürebilmek mümkün görünmektedir.

Brammer ve Pavelin (2004: 707), bir firmanın sosyal performansının önemli ölçüde firmanın paydaş çevresine ve yaptığı işlere bağlı olduğunu öne sürmektedir. Bu bağlamda, hacktivist eylemler toplumsal sorunlara dikkat çekmek için yapıldığında, eylemin hedefindeki firmaların paydaşları firmanın sosyal performansını pek önemsemiyorsa, hacktivist eylemlerin hedefine ulaşamayacağı ve firmaların kurumsal itibarlarının bu eylemlerden pek etkilenmeyeceğini söyleyebilmek mümkündür. Dolayısıyla, hacktivizm ve kurumsal itibar ilişkisi modeli tasarlanırken, durumsal faktörlere bu ilişkide bir yer verilmesi, bu ilişkilerin büyük oranda farklı senaryolarda farklı şekillerde ortaya çıkacağı düşüncesinden kaynaklanmaktadır.

Görüldüğü üzere, hacktivist eylemlerin paydaşların kurumsal itibar algılarını şekillendirme olasılıkları oldukça yüksek görünmektedir. Ancak, alan yazında hacktivist eylemlerin kurumsal itibara zarar vereceğine dair pek çok görüş olsa da, bunun hangi mekanizmalar vasıtasıyla ortaya çıkabileceğine dair bir araştırma bulunmamaktadır. Dolayısıyla bu eksikliği gidermek adına, bu çalışmada hacktivist eylemlerle paydaşların kurumsal itibar algısı arasındaki ilişkileri anlamaya yönelik geliştirilen modele göre, paydaşların hacktivist eylemin hedefindeki kuruma yönelik itibar algıları pek çok faktörden etkilenmektedir. Paydaşların; hacktivizme, büyük ölçekli işletmelere, hedefteki kurumun içinde bulunduğu sektöre yönelik genel tutumlarının, kurumsal itibar algılarını şekillendirebileceği öngörülmektedir. Ancak bu ilişkinin durumsal olduğu ve yapılan eylemin türüne göre farklı sonuçlar doğurabileceği düşünülmektedir. Ayrıca, bu ilişkide eylemi gerçekleştirenlere yönelik güven ve eylemin hedefindeki kuruma yönelik güven gibi durumsal faktörlerin de etkili olabileceği öne sürülmektedir. Modele göre, paydaşlar sözü edilen etmenlere göre hacktivist eylemi değerlendirmekte ve bu eyleme yönelik bir tutum oluşturmaktadır. Ortaya çıkan bu tutum ise, paydaşların kurumsal itibar algılarını etkilemektedir.

Kurama dair yapılan değerlendirmenin ardından, hacktivist eylemlerin firmalar açısından ne gibi faydalar sağlayabileceğine de değinmek gerekmektedir. Hacktivist eylemler, her zaman bir tehdit olarak algılanmamalı, bazen de bir fırsat

olduğunun düşünülmesi gerekmektedir. Hacktivistler, çoğunlukla zarar verici faaliyetlere girişmemekte ve firmalara uyarı olacak nitelikte sembolik eylemler gerçekleştirmektedir. Örneğin, web sitelerinin içeriğini değiştirerek veya geçici süreli bir sanal oturma eylemi düzenleyerek firmalara mesajlarını iletmeye çalışmaktadırlar. Her ne kadar firmalar açısından küçük düşürücü olabilse de, bu tip olaylara sert tepkiler vermek yerine, hacktivistlerin iletmeye çalıştıkları mesajları anlamaya çalışmak gerekmektedir. Hacktivistlerin de firmaların içinde bulunduğu çevrenin bir parçası olduğu göz önünde bulundurulmalı ve çoğu zaman firmalara toplumsal sorumluluklarını hatırlatan denetim mekanizmaları olarak da hizmet ettikleri unutulmamalıdır. Dolayısıyla, firmalar hacktivizmi ve altında yatan felsefeyi daha iyi anlayarak bir anlamda toplumun beklentilerini de daha doğru kavrayabilecektir. Bu bağlamda, hacktivistlerle kurulabilecek iyi ilişkilerin, özellikle geleceğe dair toplumsal hassasiyetlerin daha iyi anlaşılmasına aracı olabileceği düşünülmektedir.

Hacktivistler sadece toplumsal mesajları ileten aracıları değil, aynı zamanda gerçekleştirdikleri sembolik eylemlerle, firmalara güvenlik açıklarını gösteren erken uyarı sistemleri olarak da ele alınabilir. Özellikle kötü amaçlı kırıcıların saldırılarından önce firmaların bu güvenlik açıklarını kapatmaları için bir fırsat sunması, firmaların hacktivist faaliyetlerden sağlayabileceği bir diğer önemli fayda olarak görülmektedir. Nitekim, güvenlik açıkları olduğu düşünülen firmaların sıklıkla sanal saldırılara maruz kaldığı unutulmamalıdır.

Bunlara ek olarak, hacktivistler sadece sanal ortamda var olmamakta, diğer bireyler gibi onlar da aynı zamanda firmaların müşterileri, çalışanları vb. paydaş gruplarının içerisinde yer almaktadırlar. Dolayısıyla, diğer paydaşların kurumsal itibara yönelik algıları gibi, hacktivistlerin de kuruma yönelik algılarının önemli olabileceği göz önünde bulundurulmalıdır.

Sonuç olarak, hacktivist eylemlerin paydaşların kurumsal itibar algılarıyla önemli bir ilişkisi olduğu düşünülmektedir. Ancak bu algılar, eylemlerin hedefindeki firmaların davranışlarına göre de şekillenebilmektedir. Toplumsal sorumluluklarını yerine getiren firmaların hacktivist eylemlere maruz kalma olasılıkları düşük olduğundan, firmalar öncelikle bu sorumluluklarını yerine getirmeye çalışmalıdır. Bunun yanında, firmaların şeffaflığa önem vermeleri ve kamuoyundan önemli

bilgileri saklamamaları, kurumsal itibarlarına ciddi bir zarar gelmesini önleyebilecektir.

Hacktivizm sürekli olarak evrimleşen bir olgu olarak ele alınmakta ve hacktivist eylem biçimlerinin de zamanla kapsamı değişmektedir. Nitekim, hacktivizm ilk yıllarda daha çok sanal oturma eylemleri gibi ciddi zararlara yol açmayan eylemler olarak başlamasına rağmen, günümüzde bu eylemlerin yanında kurumların personeline ait kişisel bilgilerin yayınlanması gibi bazıları tarafından hacktivizmle bağdaştırılmayacağı düşünülen eylemleri de içermektedir. Bu bağlamda, hacktivist hareketlerin nasıl evrimleşeceği ve gelecekte ne gibi formlarda görülebileceği üzerine daha çok çalışma yapılması gerekmektedir.

Hacktivizm ve kurumsal itibar ilişkisi üzerine geliştirilen modele ek olarak bazı önermeler de sunulmuştur. Ancak, bu önermelerin test edilmesi gerektiği göz ardı edilmemelidir. Bu bağlamda, bundan sonra yapılacak araştırmalarda, modelde öne sürülen önermelerin test edilmesi ve hacktivist eylemlerin paydaşların kurumsal itibar algılarını nasıl etkilediğine dair bulgulara ulaşılması, modelin pratikte işleyip işlemediğini görmek adına önem kazanmaktadır. Bunlara ek olarak, tasarımlanan araştırma modeli her ne kadar kar amacı güden kuruluşlar kapsamında ele alınsa da, modelin farklı dinamikler de hesaba katılarak, kamu kuruluşları ve sivil toplum kuruluşları gibi kar amacı gütmeyen örgütlere de uyarlanabileceği düşünülmektedir.

Bu çalışmanın, hacktivizm ve kurumsal itibar ilişkisini kuramsal bir bakış açısıyla ele almasıyla ve geliştirilen model önerisiyle yazına önemli bir katkı sağlayacağı ve bu yönüyle özgün ve gelecekteki araştırmacılar ve uygulamacılar için yol gösterici bir niteliğe sahip olduğu düşünülmektedir. Bu çerçevede, geliştirilen modelden hareketle yapılacak olan gelecek çalışmalar aracılığıyla, hacktivizm ve kurumsal itibar ilişkisinin daha iyi anlaşılabileceği ve önerilen modelin geliştirilmesine de katkı yapılacağı düşünülmektedir.

KAYNAKÇA

Advisen (2012). Hacktivism: The growth and implications of this 21st century method of protest. *Advisen white paper*.

Ajzen, I. ve Fishbein, M. (2005). The influence of attitudes on behavior. *The handbook of attitudes*. *173*-221.

Akdeniz, G. (2013). Hacker etiği. Hack kültürü ve hacktivizm: Yeni bir siyaset biçimi. (ss. 9-15). İstanbul. Alternatif Bilişim Derneği.

Barnett, M. L., Jermier, J. M. ve Lafferty, B. A. (2006). Corporate reputation: The definitional landscape. *Corporate reputation review*. *9*(1): 26-38.

Beach, M. (2012). Hacktivism and the government of British Columbia. Report prepared for Information Security Branch. Office of the Chief Information Officer. Government of British Columbia.

Berens, G. ve Van Riel, C. (2004). Corporate associations in the academic literature: Three main streams of thought in the reputation measurement literature. *Corporate Reputation Review*. *7*(2): 161-178.

Beyer, J. L. (2014). The emergence of a freedom of information movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland. *Journal of Computer-Mediated Communication*. *19*(2): 141-154.

Blodgett, B. M. (2009, June). And the ringleaders were banned: an examination of protest in virtual worlds. In *Proceedings of the fourth international conference on Communities and Technologies.* 135-144. ACM.

Brammer, S. ve Pavelin, S. (2004). Building a good reputation. *European Management Journal*. *22*(6): 704-713.

Cammaerts, B. (2013). Networked Resistance: the case of WikiLeaks. *Journal of Computer-Mediated Communication*. *18*(4): 420-436.

Caruana, A. (1997). Corporate reputation: concept and measurement. *Journal of product & brand management*. *6*(2): 109-118.

Caruana, A. ve Ewing, M. T. (2010). How corporate reputation, quality, and value influence online loyalty. *Journal of Business Research*. *63*(9): 1103-1110.

Chu, H. C., Deng, D. J., Chao, H. C. ve Huang, Y. M. (2009). Next Generation of Terrorism: Ubiquitous Cyber Terrorism with the Accumulation of all Intangible Fears. *J. UCS*. *15*(12): 2373-2386.

Chun, R. (2005). Corporate reputation: Meaning and measurement. *International Journal of Management Reviews*. *7*(2): 91-109.

Coombs, W. T. ve Holladay, S. J. (2012). Fringe public relations: How activism moves critical PR toward the mainstream. *Public Relations Review*. *38*(5): 880-887.

Coombs, W. T. ve Holladay, S. J. (2012). Privileging an activist vs. a corporate view of public relations history in the US. *Public Relations Review*. *38*(3): 347-353.

Cravens, K. S. ve Oliver, E. G. (2006). Employees: The key link to corporate reputation management. *Business Horizons*. *49*(4): 293-302.

Cravens, K., Oliver, E. G. ve Ramamoorti, S. (2003). The Reputation Index: Measuring and Managing Corporate Reputation. *European Management Journal*. *21*(2): 201-212.

Davies, G., Chun, R. Da Silva, RV. ve Roper, S.(2003) Corporate Reputation and Competitiveness. Routledge.

De Castro, G. M., López, J. E. N. ve Sáez, P. L. (2006). Business and social reputation: Exploring the concept and main dimensions of corporate reputation. *Journal of business ethics*. *63*(4): 361-370.

Deephouse, D. L. (2000). Media reputation as a strategic resource: An integration of mass communication and resource-based theories. *Journal of management*. *26*(6): 1091-1112.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*. *239*-288.

Dowling, G. (2008). Creating better corporate reputations: an Australian perpective. *Melewar. TC. Facets of Corporate Identity. Communication and Reputation*. 178-196.

Ensemble, C. A. (1996). Electronic civil disobedience and other unpopular ideas.

Fitri, N. (2011). Democracy Discourses through the Internet Communication: Understanding the Hacktivism for the Global Changing. *Online Journal of Communication and Media Technologies*. *1*(2): 1-20.

Fombrun, C. J. (1998). Indices of corporate reputation: An analysis of media rankings and social monitors' ratings. *Corporate reputation review*. *1*(4): 327-340.

Fombrun, C. J. (2005). A world of reputation research, analysis and thinking—building corporate reputation through CSR initiatives: evolving standards. *Corporate Reputation Review*. *8*(1): 7-12.

Fombrun, C. J. ve Gardberg, N. (2000). Who's tops in corporate reputation?. *Corporate Reputation Review*. *3*(1): 13-17.

Fombrun, C. J., Gardberg, N. A. ve Sever, J. M. (2000). The Reputation QuotientSM: A multi-stakeholder measure of corporate reputation. *Journal of Brand Management*. *7*(4): 241-255.

Fombrun, C. J. ve Rindova, V. (1998). Reputation management in global 1000 firms: A benchmarking study. *Corporate Reputation Review*. *1*(3): 205-212.

Fombrun, C. ve Shanley, M. (1990). What's in a name? Reputation building and corporate strategy. *Academy of management Journal*. *33*(2): 233-258.

Fombrun, C. ve Van Riel, C. (1997). The reputational landscape. *Corporate reputation review*. 1-16.

Forbes. (2014). Fallout: The reputational impact of it risk. Forbes Insights.

Fryxell, G. E. ve Wang, J. (1994). The fortune corporate'reputation'index: Reputation for what?. *Journal of management*. *20*(1): 1-14.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. ve Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *Technology and Society Magazine. IEEE*. *30*(1): 28-38.

Gardberg, N. A. ve Fombrun, C. J. (2002). The global reputation quotient project: First steps towards a cross-nationally valid measure of corporate reputation. *Corporate Reputation Review*. *4*(4): 303-307.

Gatewood, R. D., Gowan, M. A. ve Lautenschlager, G. J. (1993). Corporate image, recruitment image and initial job choice decisions. *Academy of Management journal*. *36*(2): 414-427.

Gotsi, M. ve Wilson, A. M. (2001). Corporate reputation: seeking a definition. *Corporate Communications: An International Journal*. *6*(1): 24-30.

Gray, E. R. ve Balmer, J. M. (1998). Managing corporate image and corporate reputation. *Long Range Planning*. *31*(5): 695-702.

Hareli, S. ve Weiner, B. (2002). Social emotions and personality inferences: A scaffold for a new direction in the study of achievement motivation. *Educational Psychologist*. *37*(3): 183-193.

Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence*. *24*(2): 337-354.

Hutton, J. G., Goodman, M. B., Alexander, J. B. ve Genest, C. M. (2001). Reputation management: the new face of corporate public relations?. *Public Relations Review. 27*(3): 247-261.

Jordan, T. (2002). *Activism!: direct action, hacktivism and the future of society*. Reaktion books.

Jordan, T. ve Taylor, P. A. (2004). *Hacktivism and cyberwars: rebels with a cause?*. Psychology Press.

Kaulingfreks, F. ve Kaulingfreks, R. (2013). Open-access communism. *Business Ethics: A European Review*. *22*(4): 417-429.

Kenney, M. (2015). Cyber-Terrorism in a Post-Stuxnet World. *Orbis*. *59*(1): 111-128.

King, B. G. (2008). A political mediation model of corporate response to social movement activism. *Administrative Science Quarterly*, *53*(3): 395-421.

Krapp, P. (2005). Terror and play, or what was hacktivism?. *Grey Room*. (21): 70-93.

Lange, D., Lee, P. M. ve Dai, Y. (2011). Organizational reputation: A review. *Journal of Management*. *37*(1): 153-184.

Levesque, M. (2006). Hacktivism: The how and why of activism for the digital age. In *The International Handbook of Virtual Learning Environments*. 1203-1214. Springer Netherlands.

Levy, S. (2010). *Hackers: Heroes of the Computer Revolution*. O'Reilly Media, Inc.

Lin, H. S., Dam, K. W. ve Owens, W. A. (Eds.). (2009). *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*. National Academies Press.

Love, E. G. ve Kraatz, M. (2009). Character, conformity, or the bottom line? How and why downsizing affected corporate reputation. *Academy of Management Journal*. *52*(2): 314-335.

MacLeod, J. S. (1967). The effect of corporate reputation on corporate success. *Management Review*. *56*(10): 67-71.

Manion, M. ve Goodrum, A. (2000). Terrorism or civil disobedience: toward a hacktivist ethic. *ACM SIGCAS Computers and Society*. *30*(2): 14-19.

Mayer, R. C., Davis, J. H. ve Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*. *20*(3): 709-734.

Milone, M. (2003). Hacktivism: Securing the national infrastructure. *Knowledge, Technology & Policy*. *16*(1): 75-103.

Nguyen, N. ve Leblanc, G. (2001). Corporate image and corporate reputation in customers' retention decisions in services. *Journal of retailing and Consumer Services*. *8*(4): 227-236.

Paget, F. (2012). Hacktivism–Cyberspace has become the new medium for political voices. *McAfee white paper*.

Papadimitriou, F. (2006). A geography of 'Notopia' Hackers et al., hacktivism, urban cyber-groups/cyber-cultures and digital social movements. *City*. *10*(3): 317-326.

Papadimitriou, F. (2009). A nexus of Cyber-Geography and Cyber-Psychology: Topos/"Notopia" and identity in hacking. *Computers in Human Behavior*. *25*(6): 1331-1334.

Park, N. ve Lee, K. M. (2007). Effects of online news forum on corporate reputation. *Public Relations Review*. *33*(3): 346-348.

PytlikZillig, L. M., Wang, S., Soh, L. K., Tomkins, A. J., Samal, A., Bernadt, T. K. ve Hayes, M. J. (2014). Exploring Reactions to Hacktivism Among STEM College Students A Preliminary Model of Hacktivism Support and Resistance. *Social Science Computer Review. 1-19.*

Rao, H. (1994). The social construction of reputation: Certification contests, legitimation, and the survival of organizations in the American automobile industry: 1895–1912. *Strategic management journal*. *15*(1): 29-44.

Rhee, M. ve Valdez, M. E. (2009). Contextual factors surrounding reputation damage with potential implications for reputation repair. *Academy of Management Review*. *34*(1): 146-168.

Rindova, V. P. ve Fombrun, C. J. (1999). Constructing competitive advantage: The role of firm-constituent interactions. *Strategic management journal*. *20*(8): 691-710.

Rindova, V. P., Williamson, I. O., Petkova, A. P. ve Sever, J. M. (2005). Being good or being known: An empirical examination of the dimensions, antecedents, and consequences of organizational reputation. *Academy of Management Journal*. *48*(6): 1033-1049.

Roberts, P. W. ve Dowling, G. R. (2002). Corporate reputation and sustained superior financial performance. *Strategic management journal*. *23*(12): 1077-1093.

Samuel, A. W. (2004). *Hacktivism and the future of political participation* (Doctoral dissertation, Harvard University Cambridge, Massachusetts).

Sarstedt, M., Wilczynski, P. ve Melewar, T. C. (2013). Measuring reputation in global markets—A comparison of reputation measures' convergent and criterion validities. *Journal of World Business*. *48*(3): 329-339.

Schwaiger, M. (2004). Components and parameters of corporate reputation-an empirical study. *Schmalenbach business review*. *56*: 46-71.

Shamma, H. M. (2012). Toward a comprehensive understanding of corporate reputation: Concept, measurement and implications. *International Journal of Business and Management*. *7*(16): 151-169.

Shapiro, C. (1982). Consumer information, product quality, and seller reputation. *The Bell Journal of Economics*. 20-35.

Siegrist, M., Cvetkovich, G. ve Roth, C. (2000). Salient value similarity, social trust, and risk/benefit perception. *Risk analysis*. *20*(3): 353-362.

Staw, B. M. ve Epstein, L. D. (2000). What bandwagons bring: Effects of popular management techniques on corporate performance, reputation, and CEO pay. *Administrative Science Quarterly*. *45*(3): 523-556.

Taylor, P. A. (2005). From hackers to hacktivists: speed bumps on the global superhighway?. *New Media & Society*. *7*(5): 625-646.

Turban, D. B. ve Cable, D. M. (2003). Firm reputation and applicant pool characteristics. *Journal of Organizational Behavior*. *24*(6): 733-751.

Turkle, S. (2005). *The second self: Computers and the human spirit*. Mit Press.

Van Cranenburgh, K. C., Liket, K. ve Roome, N. (2013). Management responses to social activism in an era of corporate responsibility: A case study. *Journal of business ethics*. *118*(3): 497-513.

Waldron, T. L., Navis, C. ve Fisher, G. (2013). Explaining differences in firms' responses to activism. *Academy of Management Review*. *38*(3): 397-417.

Walsh, G. ve Beatty, S. E. (2007). Customer-based corporate reputation of a service firm: scale development and validation. *Journal of the Academy of Marketing Science*. *35*(1): 127-143.

Walsh, G., Beatty, S. E. ve Holloway, B. B. (2015). Measuring client-based corporate reputation in B2B professional services: scale development and validation. *Journal of Services Marketing*. *29*(3): 173-187.

Walsh, G., Beatty, S. E. ve Shiu, E. M. (2009a). The customer-based corporate reputation scale: Replication and short form. *Journal of Business Research*. *62*(10): 924-930.

Walsh, G., Mitchell, V. W., Jackson, P. R. ve Beatty, S. E. (2009b). Examining the antecedents and consequences of corporate reputation: A customer perspective. *British Journal of Management*. *20*(2): 187-203.

Wartick, S. L. (2002). Measuring corporate reputation definition and data. *Business & Society*. *41*(4): 371-392.

Weg, S. (2003). Classifying forms of online activism. Cyberactivism: Online Activism in Theory and Practice (ss. 71-95). Psychology Press.

Weigelt, K. ve Camerer, C. (1988). Reputation and corporate strategy: A review of recent theory and applications. *Strategic Management Journal*. *9*(5): 443-454.

Yang, G. (2009). Online activism. *Journal of Democracy*. *20*(3): 33-36.

http://www.fortune.com, (08.12.2015).

http://www.haygroup.com, (08.12.2015).

http://www.managementtoday.co.uk, (08.12.2015).

Metac0m. (2003). What is Hacktivism? 2.0. http://www.edshare.soton.ac.uk/8762/2/whatishacktivism.pdf, (13.10.2015).

http://www.oxforddictionaries.com, (15.01.2016).

http://www.reputationinstitute.com, (08.12.2015).

Ruffin, O. (2004). Hacktivism, from here to there. http://www.cultdeadcow.com/cDc_files/cDc-0384.php, (05.10.2015).