T.C. İSTANBUL TİCARET
ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
İŞLETME PROGRAMI

SİBER SALDIRILARIN SÜRDÜRÜLEBİLİR REKABET ÜSTÜNDEKİ ETKİLERİ

Bitirme Projesi

Yavuz Atlas
1150Y31102

İstanbul, Ocak 2016

T.C. İSTANBUL TİCARET
ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
İŞLETME PROGRAMI

SİBER SALDIRILARIN SÜRDÜRÜLEBİLİR REKABET ÜSTÜNDEKİ ETKİLERİ

Bitirme Projesi

Yavuz Atlas
1150Y31102

Danışman: Yrd. Doç. Dr. Murat Yalçıntaş

İstanbul, Ocak 2016

İÇİNDEKİLER

ÖZET

Yüksek Lisans Bitirme Projesi

SİBER SALDIRILARIN SÜRDÜRÜLEBİLİR REKABET ÜSTÜNDEKİ ETKİLERİ

Yavuz Atlas

İstanbul Ticaret Üniversitesi
Sosyal Bilimler Enstitüsü
İşletme Anabilim Dalı

Danışman: Yrd. Doç. Dr. Murat Yalçıntaş

Bu çalışmada, öncelikle siber saldırılarla ilgili bir çerçeve oluşturulmuş ardından da sürdürülebilir rekabet üstünlüğü kavramı tarihsel bağlam içerisinde farklı yaklaşımlarla incelenmiştir. Ardından iki ana siber saldırı türü olan siber casusluk ve siber sabotajın sürdürülebilir rekabet üstünlüğü sağlamış firmalara ne şekilde zarar verebileceği tartışılmıştır. Son bölümde teorik altyapısı oluşturulan meselenin gerçek hayattaki iz düşümleri incelenmiştir.

Sonuç olarak endüstri temelli yaklaşıma göre hem siber casusluk faaliyetlerinin hem de siber sabotaj faaliyetlerinin sürdürülebilir rekabet üstünde olumsuz etkisi olabileceği sonucuna varılmıştır.

Kaynak temelli yaklaşımdaysa sürdürülebilirliğin, kaynakların kopyalanamazlığına bağlanması sebebiyle siber casusluk faaliyetlerinin sürdürülebilir rekabet üstünlüğüne etkisinin sınırlı olacağı sonucuna varılmıştır. Siber sabotajsa kaynak temelli yaklaşıma göre de etkili bir saldırı biçimidir.

Anahtar Kelimeler: siber, siber saldırı, siber casusluk, siber sabotaj, rekabet, rekabet üstünlüğü, sürdürülebilir rekabet üstünlüğü

ŞEKİLLER

TABLOLAR

GİRİŞ

Bilgi sistemlerinin hızla yaygınlaşmasıyla beraber bu sistemlerin kötüye kullanımı da sürekli daha ciddi bir sorun halini almaya başlamıştır. Özellikle siber uzaydaki saldırgan tarafın lehine olan asimetrik yapı bu ortamı devletlerin de istismar etmesine yol açmıştır. Hem devlet destekli aktörlerin sahip oldukları geniş imkânlarla hem de aktivist ve suçluların bu ortamı çok etkin bir şekilde kötüye kullanımı sorunun büyümesine yol açmıştır.

Siber saldırılar devletlerden bireylere kadar çok geniş bir kitleyi hedefleyebilmektedir. Küreselleşmeyle birlikte rekabetin önemini arttırdığı bir ortamda rekabet üstünlüğü sağlamak için siber saldırı gibi kolay kullanılabilir bir araçtan faydalanmayı kimsenin düşünmemesi mümkün değildir.

Bu çalışmada siber uzay kavramları, bu ortamda saldırı gerçekleştiren aktörler ve motivasyonları incelenecektir. Ardından sürdürülebilir rekabet üstünlüğü kavramının farklı yaklaşımları incelenerek teorik çerçeve oluşturulacaktır. Bu çerçeve dâhilinde siber saldırı türleriyle, sürdürülebilir rekabet üstünlüğü yaklaşımları arasında kıyaslama yapılarak siber saldırıların sürdürülebilir rekabet üstünlüğüne etkisi tartışılacaktır. Son bölümdeyse bu konunun gerçek hayattaki iz düşümü mahiyetindeki olaylar ele alınacaktır.

1. SİBER SALDIRILAR

Tarihte siber saldırı olarak nitelendirilebilecek ilk olay 1982 yılında soğuk savaş döneminde gerçekleşmiştir. Ronald Reagan döneminin hava kuvvetleri bakanı Thomas Reed'in aktardığı bu olayda Amerika Birleşik Devletleri (ABD), Sovyetler Birliği'nin Kanada'dan bir boru hattı kontrol sistemi yazılımını çalacağını öğrenmiştir. ABD yazılımın çalınmasını engellemek yerine yazılımın bazı parametrelerinde değişiklik yapılmasını sağlamıştır. Üzerinde değişiklikler yapılmış yazılımı çalan Sovyetler Birliği bu yazılımı Trans-Siberya gaz boru hattında kullanmış ve pompa hızı ve vana ayarlarının bozulmasıyla boru hattında büyük bir patlama gerçekleşmiştir. ABD bu saldırıyla Sovyetler Birliğinin batıya gaz satışını engelleyerek ekonomik zarara uğramasını sağlamıştır **(Cornish, Livingstone, Clemente, & Yorke, 2010)**.

Her ne kadar yukarıda bahsedilen siber saldırı ABD'nin askeri istihbarat örgütü tarafından hazırlanmış kapsamlı ve maliyetli bir operasyon olsa da günümüzde siber saldırılar hem hazırlanma hem de sonuç maliyetleri açısından çok büyük farklılıklar gösterebilmektedir. Devlet destekli siber saldırılardan bilişim sistemleri hakkında elde edilen sınırlı bilgilerle gerçekleştirilen bireysel saldırılara kadar çok geniş bir yelpaze söz konusudur. Yine saldırı sonucu oluşan etki de çok küçük mali kayıplardan, firmaların iflaslarına kadar uzanabilmekte hatta can kayıplarına sebep olabilmektedir.

1.1. Siber Saldırılar ve İlgili Kavramların Tanımı

Bilişim sistemleri ve bunların kötüye kullanımı meselesi oldukça yeni olduğu için bu alanda medyanın da desteğiyle ciddi bir kavram kargaşası yaşanmaktadır. Örneğin pek çok akademik çalışma ve raporda, irili ufaklı her türlü siber saldırı, siber savaş olarak değerlendirilebilmektedir **(Sigholm, 2013)**. Bu durumda bu alanın yeni olması kadar medyanın olayları abartarak aktarmasının da etkisi olduğu söylenebilir **(Ulsch, 2014)**.

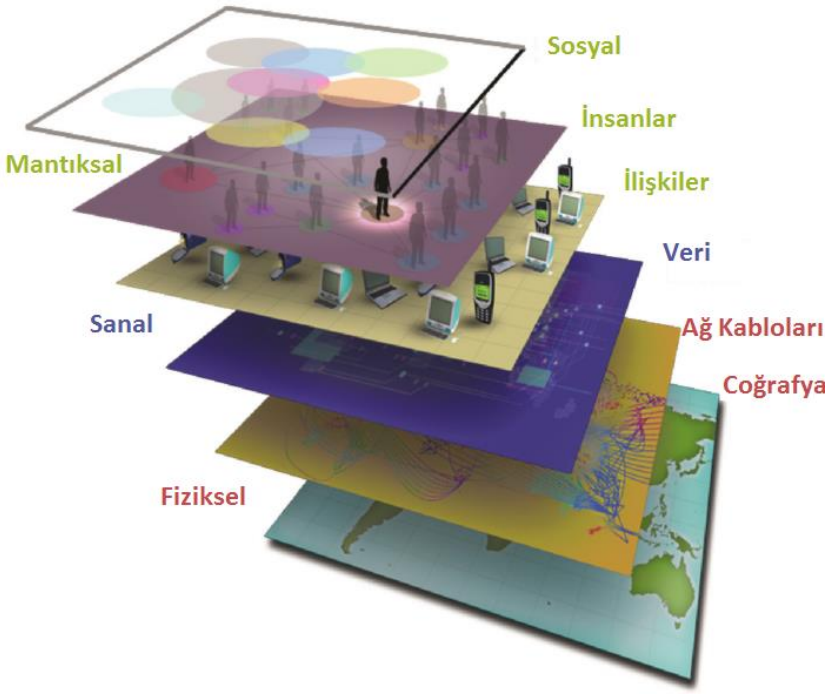
1.1.1. Siber Uzay

Tanımlanması gereken kavramlardan en önemlisi şüphesiz, tüm siber olay ve varlıkların içinde barındığı siber uzay (siber ortam) kavramıdır. Siber uzay kendine has kuralları olan, kullanım, saldırı ve korunma yöntemleri de kendine has, görece yeni bir alandır. Siber uzay verilerin depolandığı, değiştirildiği ve aktarıldığı tüm unsurları içinde barındırılan dijital ortama verilen isimdir. Bu ortam içerisinde doğrudan fiziksel güvenlikle ilgili unsurların yanında, ekonomik ve hatta sosyal unsurları da barındırmaktadır. **(UK Cabinet Office, 2011)**

Siber uzay sadece internete bağlı cihazları kapsamaz. İnternet dünya çapında coğrafyadan bağımsız olarak veri aktarımını sağlayan ve kullanıcılara interaktivite imkânı veren bir teknolojidir **(Leiner, 2009)**. Siber uzaysa internete bağlı olmayan, örneğin sadece yedekleme amaçlı kullanılan cihazları da kapsar.

Yukarıda verilen genel tanımın dışında siber uzay kavramı pek çok kaynakta askeri bakış açısıyla tanımlanmaktadır. Bu bakış açısına göre siber uzay; kara, deniz, hava ve uzaydan sonraki beşinci ve en yeni savaş alanıdır. Ancak bu yeni savaş alanı önceki dört alana göre oldukça farklı bir takım özellikler göstermektedir. **(Lord & Sharp, 2011)**

Siber uzay katmanlı bir yapıya sahiptir. Üç katmandan oluşan bu yapının ilk katmanı fiziksel katmandır. Bu katman sunucular, ağ kabloları, telefonlar gibi fiziksel cihazlar ve onların içinde bulunduğu coğrafyayı kapsar. İkinci katman olan sanal katman cihazlar arasında dolaşan veya depolanmış veri ve bu verinin işlendiği yazılımlardır. Üçüncü katmansa mantıksal katman olarak isimlendirilir. Bu katmanda gerçek insanlar ve onların siber uzaydaki kimlikleri ve ilişkileri yer alır. Örneğin e-posta hesapları ya da sosyal paylaşım sitelerindeki profiller üçüncü katmanda bulunur. **(UK Ministry of Defence, 2013)**



Şekil 1. Siber Uzayın Katmanları

Kaynak: (UK Ministry of Defence, 2013)

Siber uzayın diğer karakteristik özellikleriyse aşağıda listelenmiştir: **(Lord & Sharp, 2011)**

- Siber uzay devletler dâhil, herhangi bir güç tarafından tamamen kontrol altına alınamaz ancak bu alandaki etkinlik seviyesi arttırılabilir. Bu yönüyle karadan çok hava ve uzay savaş alanlarına benzemektedir.
- Siber uzayın coğrafya bağımlılığı çok düşüktür. Bu da coğrafyadan ve devlet sınırlarından çok az etkilenerek bu ortamda hareket edilmesini sağlamaktadır.
- Siber uzay içinde yer alan aktörlerin kimliklerini kolaylıkla saklayabildikleri bir ortamdır. Bu da siber uzay dışında var olan caydırıcılık, misilleme gibi pek çok unsuru işlevsiz veya zor uygulanır hale getirmektedir.
- Siber uzay devletler dâhil, herhangi bir güç tarafından tamamen kontrol altına alınamaz ancak bu alandaki etkinlik seviyesi arttırılabilir. Bu yönüyle karadan çok hava ve uzay savaş alanlarına benzemektedir.
- Diğer savaş alanları doğal ortamlarken siber uzay insanlar tarafından inşa edilmiş ve insanların bakımına ihtiyaç duyan bir ortamdır.
- Siber uzayda saldırgan taraf savunan taraftan avantajlı konumdadır. Bunun en büyük sebebiyse; siber ortamda savunma önlemleri oldukça maliyetliyken

saldırı için çoğu zaman bir bilgisayar ve internet bağlantısının yeterli olmasıdır.

1.1.2. Siber Güvenlik

En basit haliyle siber güvenlik, siber uzaydaki unsurların korunması olarak nitelendirilebilir. 2013 yılında yayınlanan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'na" göre siber güvenlik kavramı; siber uzaydaki unsurların saldırılardan korunmasını, tespit edilmesini, saldırılara tepki verilmesini, saldırı gerçekleştirilen sistemin saldırı öncesi haline getirmesini kapsar **(T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2013)**.

Siber güvenlik sadece bilişim sistemleriyle ilgili bir kavram değildir. Siber güvenlik siber uzaydaki her varlık ve olayı kapsar. Aslında siber güvenlikteki en önemli unsur insandır. Siber saldırıların büyük bir kısmı insanların psikolojik zafiyetlerini sömüren sosyal mühendislik yöntemleriyle gerçekleştirilir. Sosyal mühendislik saldırılarında saldırganlar insanları kandırarak onlardan kritik bilgilerini (bir sisteme giriş yapmak için kullanılan kullanıcı adı ve parola veya özlük bilgileri gibi) alır ve bu yolla oldukça maliyetsiz ve kolay bir şekilde siber uzaydaki hedeflerine ulaşmış olur **(Lorenz & Kikkas, 2012)**. Oldukça yaygın olan bu tip saldırılar siber güvenliğin insan faktörünü de kapsadığının önemli bir göstergesidir.

Siber güvenlikte temel olarak üç unsurun korunması hedeflenir: Gizlilik, bütünlük ve erişilebilirlik **(Zhou, 2005)**.

Gizlilik siber uzaydaki verilerin gizliliğini ifade eder. Bilgi her zaman için çok önemli bir güç faktörü olmuştur ama günümüzde çok daha büyük önem taşımaktadır. Özellikle gelişmiş siber saldırılar çoğunlukla kurum ve kişilerin bilgilerini çalmaya yöneliktir. Çalınan bilgi satılabileceği gibi, doğrudan çalan kişi veya kurum tarafından da kullanılabilir. Siber uzayda gizliliği korumak için en önemli yöntem verilerin şifrelenmesi ve verinin güvenli kanallardan gönderilmesidir.

Bütünlük, siber ortamdaki verilerin ve veri kaynaklarının yetkisiz kişilerce değiştirilememesini ifade eder. Siber ortamda veri kaynaklarının bütünlüğünde değişiklik gerçekleştirilerek sistemlerin olması gerekenden farklı çalışması

sağlanabilir ve bu durum saldırı gerçekleştirilen tarafa doğrudan zarar verebileceği gibi saldırgana da haksız kazanç sağlayabilir. Örneğin bir banka hesabındaki mevduat miktarını siber saldırı yoluyla arttırmak verinin bütünlüğüne yönelik saldırıdır. Bütünlüğün korunması için kullanılan yöntemler imza, yetkilendirme ve kayıt tutmadır.

Siber ortamda ihlal edilebilecek üçüncü unsursa verilerin erişilebilirliğidir. Özellikle Distributed Denial of Service (DDoS) ataklarının hedefi erişilebilirliktir. Erişilebilirliğe yönelik saldırılarda sistemlere çok fazla istek gönderilerek meşgul edilir ve bu yolla sistemlerin gerçek kullanıcılarının bu kaynaklardan faydalanması engellenir **(Geers, 2011)**. Erişilebilirliğe yönelik saldırılar, gizlilik ve bütünlüğe yönelik olanlara göre daha kolay gerçekleştirilebildiği için en sık görülen saldırı türleridir.

1.1.3. Siber Saldırı

Çalışma boyunca sıkça kullanılacak ve oldukça önemli olan bir başka terimse siber saldırıdır. Siber saldırılar siber uzaydaki unsurlara yapılan ve gizlilik, bütünlük ve erişilebilirlik unsurlarını hedef alan her türlü saldırıya verilen isimdir **(Germany Federal Ministry of the Interior, 2011)**. Burada saldıran veya savunan tarafın kim olduğunun bir önemi olmadığı gibi saldırının boyutunun ve hedefinin de bir önemi yoktur. Yukarıda sayılan unsurların en az birine yapılan her türlü saldırı siber saldırı olarak tanımlanır. Siber saldırılar ele alınırken siber uzayın fiziksel ve insani boyutu da göz önünde bulundurulmalıdır. Siber saldırılar; siber uzaydaki fiziksel unsurlar kullanılarak gerçekleştirilebileceği gibi, saldırı sonucunda fiziksel unsurlar da zarar görebilir **(United Kingdom Houses of Parliment Parliamentary Office of Science & Technology, 2011)**.

Siber saldırılarla ilgili hukuki çerçeve, 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK ile çizilmiştir. Burada "Bilişim Alanındaki Suçlar" bölümünün 243, 244, 245 ve 246. maddlerinde, bir sisteme girmek ve o sistemin işleyişini ve sistemdeki verilerin bütünlüğünü bozmak, suç kapsamında değerlendirilmiştir. Bunun dışında madde 124'teki "haberleşmenin engellenmesi", madde 132 deki "haberleşmenin gizliliğinin ihlali" ve madde 133 deki "kişiler arasındaki

konuşmaların dinlenmesi – kaydedilmesi" suçları da siber saldırı kapsamında işlenebileceği gibi siber uzaydan bağımsız da işlenebilecek suçlardır **(Ekizer, 2014)**.

1.1.4. Siber Savaş

Daha önce belirtildiği gibi siber uzayı konu alan araştırmalarda ciddi bir kavram kargaşası bulunmaktadır. Üzerinde en fazla fikir ayrılığı bulunan kavramlardan birisiyse siber savaş kavramıdır. Siber savaş kavramının tanımlanmasındaki en büyük zorluk klasik savaş tanımının siber ortama uygun olmayışıdır. Siber savaşı devletler arasında yaşanan bir savaş olarak ele almak mümkün değildir çünkü siber uzayda saldırı kapasitesi oldukça yüksek devlet dışı pek çok grup bulunmaktadır. Carl von Clausewitz'in klasik savaş tanımına göre, savaş politikanın farklı araçlarla genişletilmesidir **(Andress & Winterfeld, Cyber Warfare, Second Edition: Techniques, Tactics and Tools for Security Practitioners, 2013)**. Siber uzayda yapılan saldırılar politikanın genişletilmesi için bir araç olarak görülebilir ama yine de siber uzayda politik motivasyonla yapılan her saldırının siber savaş olarak tanımlanması da mümkün değildir. Siber ortamdaki saldırıların klasik savaş anlayışına uymamasının bir diğer sebebiyse, siber ortamda gerçekleştirilen saldırıların kolaylıkla gizlenebilmesi ve devletlerin de gerçekleştirdikleri operasyonları çoğu zaman üstlenmemesidir. Savaş iki grup arasında gerçekleşir ama siber ortamdaki saldırılar asimetriktir **(Greathouse, 2014)**. Bir başka yaklaşımsa saldırıların boyutuna bakarak siber savaş olup olmadığına karar vermektir **(Sigholm, 2013)**. Ancak bu tanımdaki sorun da siber uzayda hiçbir grupla bağlantısı olmayan bireylerin dahi bazen kendi planlarından bile büyük saldırılar gerçekleştirebilmeleridir. Bu çalışmadaysa siber savaş kavramı; en az iki grubun politik amaçlarla karşılıklı olarak birbirine yaptığı büyük kapsamlı siber saldırıları ifade edecektir.

1.2. Siber Uzaydaki Aktörler

Siber uzaydaki aktörlerin hedefleri, motivasyonları ve yöntemleri farklılıklar göstermektedir. Bu bölümde çalışmanın amacı dışına çıkmamak amacıyla sadece siber uzaydaki saldırıları belli bir amaçla gerçekleştiren aktörler ele alınacaktır. Örneğin siber güvenlik altyapılarını güçlendirmek için çalışan aktörler savunma tarafında olduğu için, kullandıkları sistemler kendilerinden habersiz bir şekilde ele

geçirilerek saldırı amaçlı kullanılan sıradan kullanıcılarsa, saldırıları kendi iradeleriyle gerçekleştirmedikleri için bu çalışmanın kapsamı dışında yer alacaktır.

Siber uzayda saldırı gerçekleştiren kişiler (siber saldırganlar) genel olarak hacker olarak adlandırılır. Aslında hacker kavramı ilk ortaya çıktığı dönemde belli bir sistemi çok iyi bilen kişi anlamına gelmekteydi. Bu terim, eskiden olumlu bir anlama sahipken günümüzde çoğunlukla siber suçlular için kullanılmaktadır. Bu çalışmadaysa hacker terimi olumlu veya olumsuz bir anlam içermeksizin siber ortamda saldırı gerçekleştirme yetkinliğine sahip kişiler için kullanılacaktır.

Hackerların sahip olduğu bilgi ve yetenekler farklılık göstermektedir. Kimi saldırganlar bu konuda zararlı yazılım geliştirebilecek kadar uzmanlaşmışken, kimileriyse ancak hazır yazılım ve yöntemleri tam olarak ne yaptıklarını bile anlamadan kullanan kişilerdir. İkinci gruptaki hackerlar "niteliksiz saldırgan" (script kiddie) olarak adlandırılmakta hatta pek çoklarına göre hacker olarak kabul edilmemektedir. Birinci gruptaki saldırganlar amaçlarına göre farklı etkileri olan saldırılar düzenleyebilirken, niteliksiz saldırganlar genellikle hedef gözetmeksizin zafiyet buldukları web sitelerinin sayfalarını değiştirerek sanal kimliklerini bilinir kılmaya ve kendilerini tatmin etmeye çalışırlar.

Çeşitli uzmanlık seviyelerindeki siber saldırganlar sahip oldukları motivasyona göre aşağıdaki gibi gruplandırılabilir.

1.2.1. Devlet Görevlileri

Siber uzayda saldırı faaliyetleri yürüten devlet görevlileri genellikle sahip oldukları geniş imkânlar ve eğitim altyapılarıyla oldukça donanımlı kişilerdir. Devlet görevlisi olan siber saldırganlar sahip oldukları güçlü bilgisayar donanımları ve uzmanlaşmaya olanak sağlayan geniş insan kaynağıyla siber uzayda çoğunlukla casusluk faaliyetleri yürütürler **(Klimburg, 2012)**.

1.2.2. Paramiliter Gruplar

Paramiliter siber gruplar devlet görevlisi olmayıp devlet tarafından kendilerine verilen görevleri yerine getiren gönüllülerden oluşur. Bu gruplara İran'daki Basij, Estonya'daki Kaitseliit ve Litvanya'daki Zemessardze içinde bulunan siber savunma

grupları örnek verilebilir **(Hopia, 2015)**. Bu gruplar içerisinde; üniversite hocaları, öğrenciler, din adamları gibi toplumun değişik kesimlerinden gönüllüler yer almaktadır **(Roscini, 2014)**. Paramiliter siber gruplarda yer alan gönüllüler çoğunlukla siber saldırılar konusunda acemi kişilerdir. Bu sebeple kompleks siber operasyonlar devlet çalışanları tarafından yürütülürken görece basit görevler paramiliter gruplar tarafından gerçekleştirilir **(Andrew Jones, 2015)**.

1.2.3. Siber Aktivistler

Siber aktivistler çoğunlukla siyasi görüşlerinin propagandasını yapmak veya ideolojik açıdan kendilerinin karşısında olan kişi ve kurumları cezalandırmak amacıyla saldırı düzenleyen hackerlardır. Siber aktivistlerin amacı çoğunlukla kurbanlarının itibar kaybetmesini sağlarken, kendi bilinirliklerini arttırmaktır. Bunun için bazen bilişim sistemlerinin hizmet vermesini engelleyen saldırılar gerçekleştirir, bazı durumlardaysa ele geçirdikleri bilgileri ifşa ederler **(UK Ministry of Defence, 2013)**. Siber aktivistlerin ideolojik amaçları da farklılık gösterir. Hayvan haklarıyla ilgili bilinç oluşturmayı hedefleyebilecekleri gibi siyasi amaçlı saldırılar da gerçekleştirebilirler **(Amir, 2015)**. Siber aktivistler her ne kadar devlet dışı aktörler olarak değerlendirilseler de istihbarat örgütlerinin bu gruplarla irtibatlı olması veya bu gruplara sızması ve yönlendirmesi de mümkündür **(AlAli, 2015)**.

1.2.4. Firmalar

Kimi firmalar da siber uzayda saldırı faaliyetleri yürütebilmektedir. Bu üç şekilde gerçekleşmektedir. Birincisi; bazı firmalar istihbarat örgütlerinin siber saldırı operasyonlarını üzerinden gerçekleştirdikleri paravan kuruluşlardır **(Andress & Winterfeld, 2013).** İkincisi; kimi firmalar devletler için doğrudan saldırı gerçekleştiren yazılımlar üretebilmektedir. İtalya merkezli Hackingteam firması buna örnek olarak gösterilebilir **(Hacking Team, 2015)**. Bazı firmalarsa rekabet üstünlüğü sağlayabilmek için siber saldırı yöntemleri kullanarak endüstri casusluğu gerçekleştirmektedir. İlk iki örnekteki aktörler devlet destekliyken sonuncusu devlet dışı aktördür.

1.2.5. Siber Suçlular

Siber suçlular siber ortamı, insanların paralarını ve bilgilerini çalarak haksız kazanç elde etmek için kullanan kişilerdir **(Sigholm, 2013)**. Siber suçlular maddi kazanç elde etmek amacıyla kredi kartı bilgilerini, kimlik bilgilerini veya bitcoin çalabilir veya bilgisayarlardaki verileri şifreleyerek fidye isteyebilirler **(Savage, Coogan, & Lau, 2015)**.

1.2.6. İç Tehditler

Son olarak ele alınacak siber saldırı aktörü iç tehditlerdir. Çalışanlar kimi zaman farkında olmadan, kimi zaman maddi çıkar elde etmek için, kimi zamansa intikam almak için çalıştıkları kuruma siber ortamda zarar verebilir. Bu zarar siber operasyonların durmasına veya yavaşlamasına yol açabileceği gibi, bilgi ifşasına da yol açabilir. Sistemlere içeriden erişimleri olduğu için iç tehditler en tehlikeli siber aktörler olarak görülmektedir. Bazı durumlardaysa işten ayrılan eski çalışanların sistemlere giriş için kullandıkları hesaplar devre dışı bırakılmadığında intikam amaçlı saldırılar gerçekleştirebilmektedirler **(Marty, 2008)**.

Siber uzayın sağladığı saldırı avantajı devletlerin de dikkatini çekmektedir. Pek çok siber aktörün farklı derecelerde devlet ilişkisi bulunmaktadır. Siber saldırganların saldırı amaçları ve devlet ilişkileri aşağıdaki tabloda yer almaktadır.

Tablo 1. Siber Aktörler, Devlet İlişkileri ve Saldırı Amaçları

Aktör	Devlet Desteği	Saldırı Amacı
Devlet Görevlileri	Var	Casusluk, Sabotaj
Paramiliter Gruplar	Var	Casusluk, Sabotaj
Siber Aktivistler	Bazı durumlarda var	Sabotaj
Firmalar	Bazı durumlarda var	Casusluk
Siber Suçlular	Yok	Sabotaj
İç Tehditler	Yok	Casusluk, Sabotaj

1.3. Amaçlarına Göre Siber Saldırı Türleri

Siber güvenlikle verinin üç unsurunun; gizliliği, bütünlüğü ve erişilebilirliğinin korunmasının amaçlanır. Siber saldırılarsa bu üç unsuru iki temel amaçla ihlal eder: Casusluk ve sabotaj.

1.3.1. Siber Casusluk

Avusturya siber güvenlik strateji belgesine göre siber casusluk bilişim sistemlerindeki verinin gizlilik unsurunu hedef alan siber saldırı türüdür **(Federal Chancellery of the Republic of Austria, 2013)**. EastWest enstitüsüyse siber casusluğu kritik veriye yetkisiz erişim sağlamayı amaçlayan gizli operasyon olarak tanımlar **(Tim Maurer, 2014)**. Bu iki tanımın ışığında ve siber güvenliğin korumaya çalıştığı unsurlar bağlamında siber casusluk terimi şu şekilde tanımlanabilir: Siber uzaydaki verinin gizlilik unsurunu hedef alan ve gizli gerçekleştirilen siber saldırılar siber casusluk olarak adlandırılır. Siber casusluk soncunda ele geçirilen veri iki şekilde kullanılabilir. Bazı durumlarda ele geçirilen veri, veriyi ele geçiren kurum tarafından doğrudan kullanılırken (süreci kopyalamak veya ar-ge çalışmasını kopyalamak gibi), bazı durumlardaysa bu veriler sadece firmaların ne yaptıkları hakkında bilgi sahibi olmak için kullanılır **(Drab, 2003)**.

Siber casusluk faaliyetleri firmalar tarafından gerçekleştirilebilmektedir. Firmaların gerçekleştirdiği siber casusluk faaliyetleri rakiplerinin ticari sırlarını veya ar-ge çalışmalarını çalmaya yönelik olabilir. Firmalar çoğu zaman ar-ge programları için yeterli kaynak bulma konusunda zorluk yaşar. Siber ortamda gerçekleştirilen casusluk faaliyetleri ar-ge çalışmalarından daha az maliyetli ve daha kısa süreli olduğu için oldukça caziptir **(Drab, 2003)**. Bunun yanında rakip firmalarda çalışan kişiler hakkında bilgi toplayarak onları transfer etmek te siber casusluk için bir başka gerekçedir.

İç tehditler de siber casusluk gerçekleştiren bir başka siber aktördür. Bu kişiler çalıştıkları kurumlardan çaldıkları bilgiyi başka firma veya devletlere satarak maddi çıkar elde ederler. Bunun dışında neyin gizli neyin anonim bilgi olduğunu kavrayamayan çalışanlar da istemeden firmalarıyla ilgili ticari sır niteliğinde bilgileri başkalarıyla paylaşabilir.

Siber casusluk faaliyetleri en çok devletler tarafından tercih edilir. Devletler tarafından gerçekleştirilen siber casusluk saldırıları diğer devletlerin askeri sırlarını çalmaya yönelik olabileceği gibi siyasi amaçlı da gerçekleştirilebilir **(Moore, 2010)**. Bununla birlikte devlet görevlileri başka ülkelerdeki firmaların ticari sırlarını çalarak kendi ülkelerindeki firmalara ekonomik üstünlük sağlamayı da hedefleyebilir.

Bu noktada ticari sır kavramının hangi varlıkları kapsadığının doğru anlaşılması önemlidir. Farklı ülkelerde ticari sır kavramının kapsamı değişiklik göstermekle birlikte bu kavram Türkiye'de Başbakanlık tarafından 2008 yılında TBMM'ye gönderilen "Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı" ile tanımlanmıştır. Buna göre ticari sır; bir ticarî işletme veya şirketin faaliyet alanı ile ilgili yalnızca belirli sayıdaki mensupları ve diğer görevlileri tarafından bilinen, elde edilebilen, özellikle rakipleri tarafından öğrenilmesi halinde zarar görme ihtimali bulunan ve üçüncü kişilere ve kamuya açıklanmaması gereken, işletme ve şirketin ekonomik hayattaki başarı ve verimliliği için büyük önemi bulunan bilgi ve belgeleri ifade eder. Bu bilgi ve belgelerse aşağıdaki gibidir **(T.C. Başbakanlık, 2008)**:

- iç kuruluş yapısı ve organizasyonu
- malî, iktisadî, kredi ve nakit durumu,
- araştırma ve geliştirme çalışmaları
- faaliyet stratejisi
- hammadde kaynakları
- imalatın teknik özellikleri
- fiyatlandırma politikaları
- pazarlama taktikleri ve masrafları
- pazar payları
- toptancı ve perakendeci müşteri potansiyeli ve ağları
- izne tâbi veya tâbi olmayan sözleşme bağlantıları

Dolayısıyla ticari fayda sağlamayı amaçlayan siber casusluk faaliyetlerinin yukarıda sayılan bilgileri hedef aldığı söylenebilir. Her ne kadar siber casusluk görece yeni bir kavram olsa da devletlerin fiziksel dünyada casusluk faaliyetleri gerçekleştirmesi çok daha eskiye dayanmaktadır. Bu bağlamda siber casusluk için, fiziksel casusluğun

siber ortama genişlemiş hali olduğu söylenebilir **(Cornish, Livingstone, Clemente, & Yorke, 2010)**. Devletler siber casusluğu geleneksel casusluk yöntemleriyle birleştirerek te kullanabilir **(Lewis J. A., 2013)**.

1.3.2. Siber Sabotaj

Almanya ve Avusturya'nın siber güvenlik stratejilerine göre siber sabotaj, siber uzaydaki sistemlerin bütünlük ve erişilebilirliğini etkileyen siber saldırı türleridir **(Germany Federal Ministry of the Interior, 2011)**. Bu tanım çoğunlukla doğru olsa da eksik kaldığı durumlar da bulunmaktadır. Kurum ve kişilere sabotaj amaçlı saldırılar düzenleyen siber aktivistlerin kullandığı saldırı yöntemleri arasında sistemlerden bilgi çalıp bunu ifşa etmek te bulunmaktadır. Dolayısıyla siber sabotajın bütünlük ve erişilebilirlikle birlikte gizliliği de hedef aldığı söylenebilir.

Özellikle siber aktivistler siber sabotaj yöntemlerini çok sık kullanır. Verileri ifşa etmelerinin yanı sıra verilerin erişimini engelleyen hizmet dışı bırakma saldırıları (DoS) siber aktivistlerin en sık kullandığı yöntemdir. Kurum ve kişilerin itibarına zarar vermeyi amaçlayan web sitesi tahrifatı (defacement) saldırılarıysa verilerin bütünlüğünü bozar.

Siber suçlular da verilerin bütünlüğünü bozmaya yönelik sabotaj yöntemlerini sıkılıkla tercih etmektedirler. Özellikle son dönemlerde sıklıkla tercih edilen fidye yazılımlarıyla (Ransomware) erişebildikleri sistemlerdeki dosyaları şifreleyen siber suçlular ancak istedikleri ücret ödenirse şifreli dosyaları açacak parolayı vermektedir **(Bromium, 2014)**. Bunun yanında kişilerin banka hesap bilgilerini ele geçiren siber suçlular, kurbanlarının hesaplarından kendi hesaplarına para transfer ederek veya girdikleri bilgisayarlardaki bitcoinleri kendi hesaplarına transfer ederek te maddi kazanç elde edebilmektedir.

Siber sabotaj için verilebilecek diğer örnekse devlet görevlilerinin gerçekleştirdiği operasyonlardır. Devlet destekli siber sabotajlar çoğunlukla kritik bir kurumun çalışmasını engellemeye yönelik son derece kompleks saldırılardır. Bu tip sabotajlar bazen bir enerji nakil hattında patlamaya sebep olurken bazense bir nükleer santralin çalışmasını durdurabilmektedir. Nadir durumlardaysa devletler ele geçirdikleri gizli bilgileri ifşa ederek sabotaj gerçekleştirirler.

İç tehditlerin uyguladığı sabotaj yöntemiyse genellikle erişilebilirlik ve veri bütünlüğüne yönelik olarak gerçekleşmekle birlikte zaman zaman gizliliği de hedef alabilmektedir. İyi niyetli iç tehdit siber sabotaj saldırıları (sisteme hatayla zarar verenler) genellikle bir hizmetin yanlış çalışmasını sağlayarak erişilebilirlik ve veri bütünlüğünü ihlal etmektedirler. Bununla birlikte Edward Snowden olayında görüldüğü gibi veri ifşasında bulunarak sabotaj gerçekleştiren iç tehditler de bulunmaktadır **(Macaskill & Dance)**.

Yukarıdaki incelemenin sonucunda siber sabotaj eylemlerinde temelde aşağıdaki amaç ve yöntemlerin benimsendiği söylenebilir:

- Veri ifşası yöntemiyle itibara zarar verme
- Şantaj sebebiyle veya çıkar sağlamak için verinin satılması
- WEB sitesi tahrifatıyla itibara zarar verme
- Verileri şifreleyerek fidye isteme
- Banka hesaplarından ve bitcoin cüzdanlarından para transferi
- DoS saldırılarıyla sistemleri kullanılamaz hale getirerek maddi kayba sebep olma
- Fiziksel sistemlerin işleyişini değiştirmek amaçlı veride değişiklik
- Çalışanların yanlışlıkla sistemin işleyişini bozması

2. SÜRDÜRÜLEBİLİR REKABET ÜSTÜNLÜĞÜ

Bu bölümde stratejik yönetim anlayışındaki tarihsel değişimle birlikte rekabet üstünlüğü kavramının ortaya çıkışı, evrimi ve bu alandaki farklı yaklaşımlar genel hatlarıyla ele alınacaktır.

2.1. Stratejik Yönetimin Tarihsel Evrimi ve Rekabet Üstünlüğü

2.1.1. Stratejik Planlama Dönemi

Stratejik yönetimde rekabet kavramının kullanımı ancak 1980 yılından sonra olmuştur. Bunun öncesinde stratejik planlama anlayışı hâkimdir. 1960 yılından 1980 yılına kadar süren stratejik planlama döneminin en önemli iki yönlendiricisi Kenneth Richmond Andrews ve Harry Igor Ansoff'tur **(Barca, 2009)**. Andrews ve Ansoff'un ortaya koyduğu çalışmalarda rekabet üstünlüğü kavramına hiç değinilmemiş ve stratejik planlama kavramı tercih edilmiştir. Her ne kadar 1980 yılından itibaren stratejik planlama kavramı yerine başka kavramlar tercih edilmeye başlamış olsa da stratejik planlama anlayışı varlığını günümüze kadar devam ettirmiştir. Özellikle kamu kurumları çoğunlukla stratejik planlama yaklaşımını kullanmaktadır. **(Göral, 2009)**.

Kenneth Richmond Andrews'un Harward Üniversitesi'ndeki üç profesörle beraber stratejik planlama için geliştirdiği SWOT analizi yöntemi günümüzde hala sıklıkla tercih edilmektedir. SWOT analizi yöntemi kurumların iç faktörlerinin yanında, dış çevresini de göz önünde bulunduran ilk modellerden birisidir. Bu yöntem, kurumların kendi bünyelerinde barındırdıkları güçlü ve zayıf yanlarıyla, dış ortamdaki fırsat ve tehditleri ortaya koymak suretiyle planlama yapmasına olanak tanır.

Harry Igor Ansoff'un ortaya attığı boşluk analizi yöntemiyse bir kurumun bugünkü konumundan hedeflenen konumuna nasıl ulaşabileceğinin planlaması için kullanılan bir modeldir. Bu modelde öncelikle gelecekte varılması istenen hedef kararlaştırılır ve mevcut konumla gelecekteki konum arasındaki boşluk belirlenir. Daha sonra bu boşluğu doldurmak için ihtiyaç duyulan eylemler kararlaştırılıp bu eylemlerle

hedeflenen noktaya ne kadar yaklaşılabileceği hesaplanır. Eğer bu hesap sonucunda hedeflere yeterince yaklaşılamayacağı bulunursa eylem kararlaştırma adımına tekrar dönülür **(Barca, 2009)**.

Stratejik planlama yaklaşımında daha çok işletmenin dış çevresi analitik olarak incelenirken, yönetim tarzı, örgüt kültürü, liderlik gibi iç faktörlerine odaklanılmamıştır. Bu yaklaşımda çoğunlukla istatistik yöntemleri kullanılarak gelecek tahmininde bulunmaya çalışılmıştır **(Ülgen & Mirze, 2013)**.

2.1.2. Rekabet Üstünlüğü Sağlamada Endüstri Temelli Yaklaşım

1970'lerin ortalarından itibaren uzak doğu ülkelerinin Batılı ülkelerdeki etkinliği 1980'li yıllarda ciddi bir başarıya dönüştü. Uzak doğulu işletmelerin batı pazarını domine etmeye başladığı bu dönem batılı devletlerin pazardaki etkinliklerini özelleştirmelerle azaltması neticesinde batı pazarını rekabetin daha da önemli olduğu bir ortam haline getirdi. Bu süreçte Micheal Porter'ın yazdığı Rekabet Stratejisi isimli kitapla birlikte rekabet stratejisi anlayışı dönemi başlamıştır **(Barca, 2009)**. Ama özellikle Porter'ın 1985 yılında yazdığı Rekabet Üstünlüğü isimli kitabında "rekabet üstünlüğü" kavramını kullanmasıyla birlikte stratejik yönetim kavramı yerine daha çok rekabet üstünlüğü kavramı kullanılmaya başlamıştır **(Göral, 2009)**.

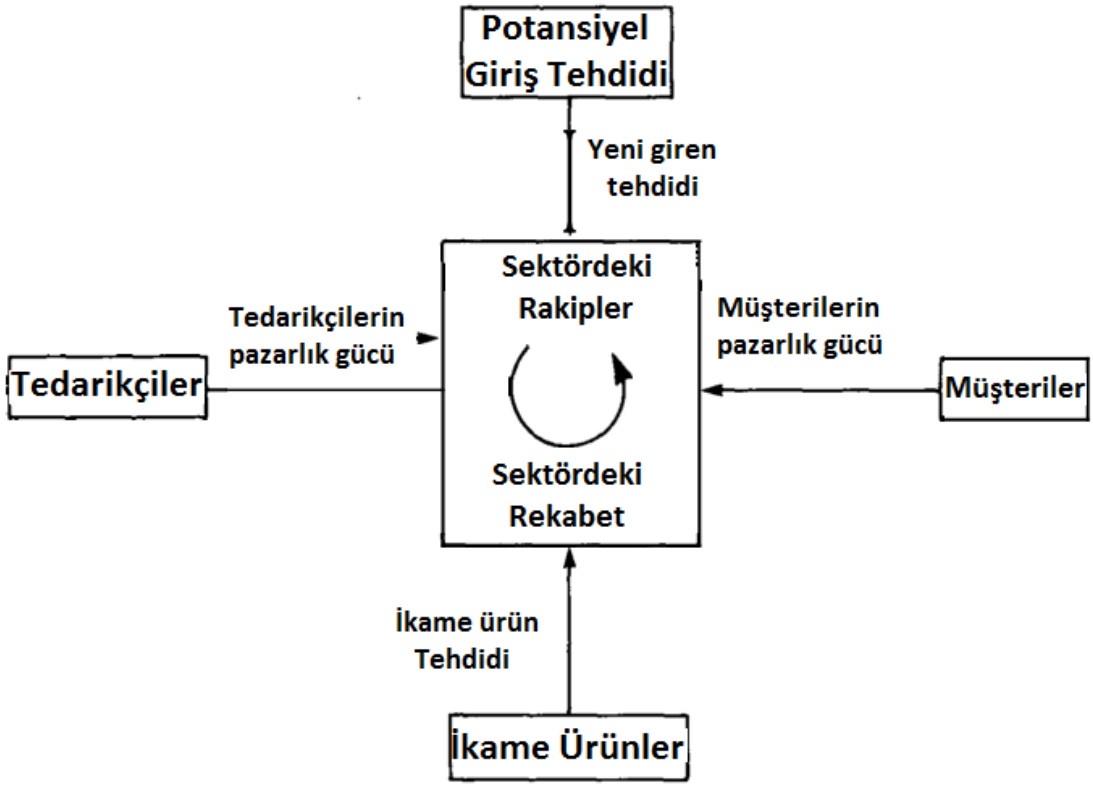
Porter'ın ortaya koyduğu modele göre işletmenin uygulayacağı strateji işletmenin faaliyet gösterdiği sektörle uyumlu olmak durumundadır. Bunun için öncelikle sektördeki rekabetin yapısını belirleyen beş kuvvet incelenmelidir. Porter'ın beş rekabet kuvveti aşağıdaki gibidir **(Porter, 1998)**:

1. **Potansiyel Giriş Tehdidi:** Bir sektöre giriş bariyerleri ne kadar yüksekse ve sektördeki mevcut işletmelerin yeni girenlere göstereceği tepki ne kadar büyükse sektöre yeni girecek rakiplerin tehdidi de o kadar düşüktür. Sektöre giriş tehdidinin boyutunu belirleyen faktörler aşağıda verilmiştir.

    - Beklenen misillemeler
    - Ölçek ekonomileri
    - Ürün farklılaştırma

- Sermaye gerekleri
- Dağıtım kanallarına erişim
- Ölçekten bağımsız maliyet dezavantajları
- Devlet politikaları

2. **Güçlü Müşteriler:** Müşteriler sahip oldukları pazarlık gücüyle sektördeki mal ve hizmetlerin fiyatını düşürebilirler.
3. **Tedarikçiler:** Sektördeki tedarikçilerin güçlü olması sektör için risk oluşturabilir. Tedarikçiler sahip oldukları güçle ürünlerin fiyatlarını yükseltebilir veya kalitelerini düşürebilir.
4. **İkame ürünler:** İkame ürünler sektördeki ürünlerin fiyatlarının üst sınırını belirleyen unsurlardan birisidir.
5. **Sektördeki Mevcut İşletmeler Arasındaki Rekabet:** Sektörün karlılığı sektördeki mevcut işletmeler arasındaki rekabetin yoğunluğu ölçüsünde düşer. Çünkü rekabet, müşteriye daha ucuz ve farklı ürün satılmasını gerekli kılar ve bu da sektörün karlılığını düşürür.



Şekil 2. Rekabeti Etkileyen Beş Kuvvet

Kaynak: (Porter, 1998)

Sektördeki beş rekabet kuvveti incelenerek dış çevre hakkında fikir sahibi olunduktan sonra işletmenin hangi stratejiyle rekabet edeceği kararlaştırılır. Porter'a göre işletmelerin rekabet için benimseyebileceği üç jenerik strateji bulunmaktadır.

Üç jenerik strateji, rekabet üstünlüğünü amaçlayan firmaların sektördeki beş kuvvete karşı alması gereken tedbirler ve beş kuvvetten istifade etmek için kullanılabilecek genel stratejilerdir. Sektördeki beş kuvvetin analizi yapıldıktan sonra bu stratejilerden birisi izlenmelidir.

1. Maliyet Liderliği Stratejisi

İşletmelerin rakiplerinden daha düşük maliyetle mal ve hizmet üretimi yaparak rekabet etmesidir. Maliyet liderliğine sahip işletmeler beş rekabet kuvvetinden rakiplerine göre daha az etkilenirler çünkü maliyet liderliği çoğu zaman sektöre giriş bariyerlerini yükselterek potansiyel rakiplerin işini zorlaştırır. Tedarikçilerin fiyat yükseltmesine karşın rakiplerden daha az etkilenirler ve ikame ürünler karşısında da çoğu zaman avantajlı durumdadırlar **(Porter, 1998)**.

Maliyet liderliği sağlamak için çoğunlukla aşağıda sıralanan kaynak ve kabiliyetlere ihtiyaç duyulur **(Porter, 1998)**:

- Rakiplerden daha yüksek pazar payı
- Hammaddelere rakiplerden daha az maliyetle erişim
- Verimli tesislerin kurulması
- Tecrübeden faydalanarak maliyeti düşürme
- Sıkı harcama denetimi
- Küçük müşteriden kaçınma
- Ar-Ge, hizmet, satış, reklam gibi alanlarda maliyet düşürme
- Yöneticilerin harcamaları düşürme konusuna önem vermesi

Maliyet liderliği stratejisinin riskleriyse;

- Teknolojik değişimler daha önceki yatırımları etkisiz kılabilir

- Sektöre yeni giren firmaların düşük maliyetlerle maliyet liderliği sağlayan kaynakları kopyalaması veya tesis yatırımlarıyla düşük maliyet sağlaması
- Pazardaki değişimi maliyetlere odaklanıldığı için görememek ve müşterinin ihtiyacını anlayamamak
- Sektördeki rakiplerin marka imajlarına karşın yeterince fiyat düşürememek

2. Farklılaştırma Stratejisi

Farklılaştırma stratejisi uygulayan işletmeler piyasaya rakiplerinden farklı ürünler sunarak üstünlük sağlamaya çalışır. Bu farklılığın üstünlük sağlanmaya çalışılan sektöre özel olması beklenir. Farklılaştırma stratejisi maliyetleri göz ardı etmez, sadece ürün farklılaştırmayı birinci hedef olarak görür. Bununla birlikte farklılaştırma çoğu zaman üretim maliyetinin artmasına sebep olduğu için fiyatların da yükselmesine sebep olur **(Minarik, 2007)**.

Farklılaştırma stratejisini başarıyla uygulayan işletmeler çoğunlukla marka sadakati oluşturdukları için sektördeki rekabetten diğer işletmelere göre daha az etkilenir. Sektöre girmeyi düşünen potansiyel rakiplerin de öncelikle müşteri sadakatini aşmaları gerektiği için sektöre giriş bariyerini yükseltir. Bunun yanında farklılaştırılmış ürünler çoğunlukla yüksek fiyatlarla satıldığı için tedarikçilerin maliyetleri yükseltmesine karşı rakiplere göre daha dirençlidirler. Aynı zamanda müşterilerin de pazarlık gücü azdır çünkü aynı kalitede ürünü bulmaları mümkün değildir ve bu durum ikame ürünlerin de farklılaştırılmış ürünler karşısında etkisini azaltır **(Porter, 1998)**.

Farklılaştırma stratejisinde farklılaştırmanın tek bir alan yerine farklı boyutlarda yapılması tercih edilir. Ürünleri farklı kılabilecek bazı özellikler; tasarım ve marka itibarı, teknoloji, ürünün özellikleri, müşteri hizmetleri ve bayi ağıdır. Bu sayılanlar dışında kalan başka özellikler de ürünlerin farklılaşmasını sağlayabilir.

Farklılaştırma stratejisini başarıyla uygulayan işletmeler çoğunlukla aşağıdaki kaynak ve kabiliyetlere sahiptir **(Porter, 1998)**:

- Güçlü pazarlama yeteneği

- Araştırma ve ürün geliştirme yeteneği
- Güçlü müşteri desteği
- Kalite veya teknoloji konusunda itibar
- Güçlü iletişim
- Ar-Ge, ürün geliştirme ve pazarlama fonksiyonları arasında güçlü koordinasyon
- Yüksek kaliteli iş gücü

Farklılaştırma stratejisini riskleriyse şunlardır:

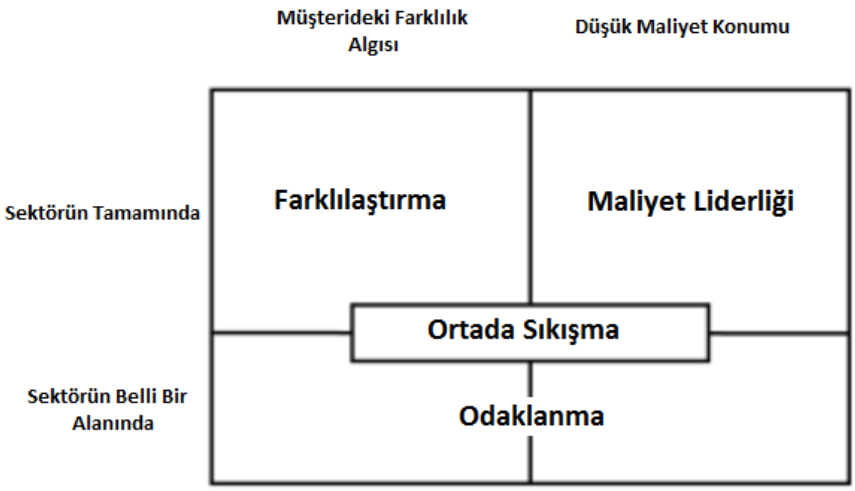
- Yeterince farklı ürün ortaya konulamadığı için müşterilerin düşük maliyetli mal ve hizmet sunan rakipleri tercih etmesi
- Müşterilerin farklılaştırma ihtiyaçlarının düşmesi
- Taklit ürünlerin farklılık algısına zarar vermesi

3. Odaklanma Stratejisi

Rekabetin şiddetli ve rekabetçi sayısının çok olduğu sektörlerde orta ve küçük ölçekli işletmelerin rekabet üstünlüğü sağlayabilmeleri çok zordur. Bu durumdaki işletmeler odaklanma stratejisini tercih edebilmektedir **(Ülgen & Mirze, 2013)**.

Odaklanma stratejisinde işletmeler bütün sektöre hitabeden stratejiler geliştirmek yerine sektör içerisindeki belli bir müşteri grubuna, iş koluna veya coğrafik pazara odaklanır. Bu sayede sadece özel bir grubun ihtiyaçları dikkate alındığı için bu grubun ihtiyaçları tüm sektöre hizmet veren firmalardan daha iyi karşılanabilir. Yine belli bir gruba yönelik üretim yapmak bazı durumlarda maliyeti de düşürebilir.

Odaklanma stratejisi tek başına uygulanabilen bir strateji değildir. Bu stratejiyi uygulayan firmalar hedefledikleri daraltılmış pazarda düşük maliyet stratejisi veya farklılaştırma stratejilerinden birini uygular. Dolayısıyla odaklanma stratejisi beş rekabet gücüne karşı maliyet liderliği veya farklılaştırma stratejilerinin avantajlarına sahiptir. Bunun yanında işletmeler bu stratejiyle daha küçük alanlarda rekabet şansı yakaladıkları için kendilerine rekabetin az olduğu ve ikame ürünlerin etkisinin az olduğu alanlar bulma konusunda da daha avantajlı konumdadır **(Porter, 1998)**.



Şekil 3. Üç Jenerik Strateji

Kaynak: (Porter, 1998)

Porter'a göre bu temel stratejilerden sadece biri seçilmelidir. Bu stratejileri aynı anda uygulamaya çalışmak "arada sıkışmaya" sebep olacağı için işletmelerin başarısızlığına yol açacaktır. Bununla birlikte bu stratejilerin uygun şekilde beraber kullanılmasının başarılı sonuç vereceğini iddia eden çalışmalar da mevcuttur **(Soyer, 2007)**.

Üç jenerik strateji, sektördeki beş kuvvet analiz edildikten sonra, beş kuvvete karşı hangi stratejik yöntemlerin izleneceğiyle ilgili bir çerçeve oluşturur. İşletmeler bu süreci doğru yürüterek seçilen jenerik strateji üzerinden rekabet üstünlüğü sağlamayı hedefler.

2.1.3. Rekabet Üstünlüğü Sağlamada Kaynak Temelli Yaklaşım

1990 yılından günümüze temel yetkinliklere dayalı strateji anlayışı hâkim olmuştur. Bu dönemdeki strateji anlayışı, daha çok işletmelerin onları rakiplerinden üstün kılacak yetkinlik ve kaynaklarına yoğunlaşmıştır. Bu anlayış rekabet stratejileri anlayışının öne sürdüğü sektörel güçlerin strateji üzerindeki etkisini göz ardı etmemekle birlikte işletmelerin kendi bünyelerindeki varlıkları asıl belirleyici olarak görür. Bu anlayışın öncüleri Betis Wernerfelt, G. Hamel, C.K. Prahalad, J. Barney ve R.P. Rumelt'dir **(Barca, 2009)**.

Rekabet üstünlüğünün sahip olunan kaynaklarla sağlanabileceğini öne süren Barney'e göre bir kaynağın rekabet üstünlüğü sağlayabilmesi için o kaynağın rakipler tarafından hemen kopyalanamaması gerekir. Burada sadece mevcut rakiplerden değil aynı zamanda potansiyel rakiplerden de söz edilmektedir.

Kaynak temelli yaklaşımda kaynak kavramıyla ifade edilen sadece fiziksel kaynaklar değildir. İşletmelerin verimliliğini arttırabilecek her türlü özelliği kaynak olarak ele alınmaktadır. Bunlar içerisinde işletmelerin sahip olduğu fiziksel varlıklarla birlikte, örgütsel süreçler, bilgi, itibar gibi özellikler de bulunmaktadır. Bir işletmenin sahip olabileceği ve işletmenin verimliliğini arttırabilecek kaynaklar üç ana başlıkta gruplandırılabilir **(Barney, 1991)**:

- **Fiziksel Kaynaklar**

  İşletme içerisinde kullanılan cihazlar, teknoloji, işletmenin coğrafik konumu, hammaddelere ulaşım gibi kaynaklar fiziksel kaynaklardır. Fiziksel kaynaklar bazı durumlarda kaynağın sahibi olan işletmeye özeldir. Bu durumlarda kaynağın kopyalanması çok zordur. Örneğin bir firmanın dağıtım kanallarının veya sahip olduğu avantajlı coğrafik konumun kopyalanması çoğunlukla zordur **(Das & Teng, 2000)**.

- **İnsan Kaynakları**

  Yönetici ve çalışanların almış olduğu eğitimler, sahip olduğu tecrübe ve bilgi, kısaca insan kaynakları işletmelerin verimliliğini arttırabilir **(Barney, 1991)**. Aynı teknolojiyi kullanan iki firmadan operasyon yeteneği güçlü çalışanlara sahip olan yani insan kaynağı daha iyi olan rekabet üstünlüğü kazanacaktır. Çalışanların sahip olduğu operasyon kabiliyetleri, sahip olduğu bilgiyle ilişkilidir **(Boxall, 1998)**.

  Çalışanların kendileri başka bir işletmeye gidebilse de onlardan bağımsız olarak bilgilerinin başka bir işletmeye gitmesi her zaman mümkün değildir. Çalışanların sahip olduğu ve kullandığı bilgi ikiye ayrılır: Açık ve kapalı bilgi. Açık bilgi kolaylıkla aktarılıp depolanabilen bir bilgi türüdür. Diğer taraftan kapalı bilgiliyse insanlar tarafından bir işi uzun süre yaparak kazanılır. Buna tecrübe de denebilir. İnsan kaynaklarının rekabet üstünlüğü sağlamasındaki en

önemli sebep kapalı bilgi sahibi çalışanlardır. Bu tip bilgi, ona sahip kişi işyerinden ayrıldığında onunla birlikte gider **(Yiğit & Özyer, 2011)**.

- **Örgütsel Kaynaklar**

Her türlü formal ve informal süreç ve işletme içinde ve dışındaki informal ilişkiler, kurum kültürü ve işletmedeki örgütsel bilgi örgütsel kaynak olarak ele alınır **(Barney, 1991)**.

Örgütsel kaynaklar kolaylıkla kopyalanamayan türde kaynaklardır. Örneğin bir örgütsel kaynak olan kurum kültürü bir işletmedeki çalışanların büyük kısmının kabul ettiği değer ve davranışlardır. Kurum kültürü işletmedeki çalışanlar ve müşterilerin varlılarıyla ortaya çıktığı için diğer işletmeler tarafından kopyalanamaz **(López, Salazar, Castro, & Sáez, 2006)**.

Örgütsel kaynaklar üzerinden rekabet üstünlüğü sağlayan işletmeler çalışanları işten ayrılsa bile rekabet üstünlüğü sağlayan bilgiyi işletme içinde tutmaya devam eder. Örneğin bazı futbol kulüplerinin oyuncuları ve hatta teknik direktörleri değiştiği halde uzun yıllar diğer kulüplere rekabet üstünlüğü sağladığı bir gerçektir. Bu kulüplerin en önemli özelliği kulüp içinde çalışan kişiler değişirken oyun sisteminin aynı kalması ve yeni gelenlere bu sistemin aktarılmasıdır **(Ludewig & Sadowski, 2009)**.

Bu kaynakların birbirileriyle hiçbir ilgisi olmadığı durumlar olduğu gibi birbirilerinin ikamesi oldukları veya birbirilerini tamamladıkları durumlar da bulunabilir. Örneğin bir işletmede çalışanlara o işletmeye özel üretilmiş bir makinenin eğitimi veriliyor olabilir. Bu durumda işletmenin insan kaynağı ve fiziksel kaynağı arasında bir tamamlayıcılık ilişkisi söz konusudur **(Bryant-Kutcher, Jones, & Widener, 2008)**.

Barney'nin kaynak kavramına yaklaşımında fiziksel kaynakların dışında insan kaynakları ve örgütsel kaynakların da bulunması, kaynak kavramıyla yeteneklerin de kastedildiğini göstermektedir. Buna rağmen kaynak ve yetenek ayrımı yapan yaklaşımlar da bulunmaktadır. Örneğin Grant'a göre yetenek bir işletmenin sahip olduğu kaynaklardan faydalanarak bir takım süreçleri yürütebilmesi ve bu sayede hedeflediği bir amaca ulaşmasıdır. Bu yaklaşıma göre ancak yetenekler ve kaynaklar

beraber kullanılırsa rekabet üstünlüğüne ulaşılabilir **(Grant, 1991)**. Bu çalışmadaysa kaynak kavramı yetenekleri de kapsayacaktır.

2.2. Sürdürülebilir Rekabet Üstünlüğü

1990'lı yıllardan itibaren yapılan çalışmalarda stratejik yönetim ve rekabet üstünlüğü kavramları yerine çoğunlukla sürdürülebilir rekabet üstünlüğü kavramı kullanılmıştır. Bu alanda çalışmalar yapan pek çok insanla birlikte Michael Porter dahi ilk baskısı 1985 yılında yapılan Rekabet Üstünlüğü kitabında "rekabet üstünlüğü" kavramını kullanırken aynı kitabın 1998 yılında yapılan baskısında bu kavramın yerini "sürdürülebilir rekabet üstünlüğü" kavramı almıştır **(Göral, 2009)**. Jay Barney'nin 1991 yılında yazdığı "Firm Resources and Sustained Competitive Advantage" isimli makalesinin de merkezinde sürdürülebilir rekabet üstünlüğü kavramı yer almaktadır **(Barney, 1991)**.

Rekabet üstünlüğünün sürdürülebilir hale getirilmesi konusunda temelde iki yaklaşım benimsenmektedir.

2.2.1. Sürdürülebilir Rekabet Üstünlüğü Sağlamada Endüstri Temelli Yaklaşım

Porter'ın öncüsü olduğu endüstri temelli sürdürülebilir rekabet üstünlüğü yaklaşımına göre bir işletmenin rekabet üstünlüğünün sürdürülebilir olması zamanla ilgili bir durumdur. Eğer işletmenin rekabet üstünlüğü yeterince uzun sürebilmişse bu işletmenin sürdürülebilir rekabet üstünlüğü sağladığı söylenebilir. Porter söz ettiği zamanın ne kadar olduğunu belirtmemiştir **(Barney, 1991)**.

Bununla birlikte Porter rekabet üstünlüğünün uzun sürmesini yani sürdürülebilir olmasını sağlayan üç koşuldan bahseder. Bu koşullar aşağıdaki gibidir **(Seviçin, 2009)** :

1. **Üstünlüğün kaynağı**: Rekabet üstünlüğünün maliyet liderliğiyle mi yoksa farklılaştırmayla mı elde edildiği sürdürülebilirliğin süresini etkiler. Rekabet üstünlüğü sağlamada jenerik stratejilerin hiyerarşik bir yapısı olduğu söylenebilir ve bu yapıda farklılaştırma stratejisi maliyet liderliği stratejisine

göre daha üstündür. Dolayısıyla farklılaştırma stratejisi çoğu zaman maliyet liderliğine göre daha sürdürülebilirdir.

2. **Farklı üstünlük kaynaklarının sayısı**: Rekabet üstünlüğü ne kadar az kaynak ve kabiliyetle elde edilirse sürdürülebilirliğin sağlanması o derece zorlaşır. Çünkü bir sebeple rekabet üstünlüğü sağlayan kaynak ve kabiliyetler eski etkisini kaybedebilir. Örneğin sadece bir hammaddeye yakınlıkla sağlanmış rekabet üstünlüğü o maddenin ikamesinin bulunmasıyla ortadan kalkabilir. Bu sebeple üstünlük kaynakları ne kadar fazlaysa rekabet üstünlüğü de o kadar uzun sürer.

3. **Sürekli yenilik ve gelişim**: Üstünlük kaynak ve kabiliyetleri sürekli geliştirilmelidir. Rekabet üstünlüğü sağlayan firmaların rekabet üstünlüğü sağlayan kaynak ve kabiliyetlerin mevcut durumuyla yetinmesi büyük bir hatadır. Örneğin Ar-Ge faaliyetleriyle geliştirilmiş bir makineyle daha hızlı üretim yapan ve bu yolla maliyet liderliği yakalayan bir işletmenin bu kaynakla yetinmesi sürdürülebilirliği engelleyecektir. Çünkü eninde sonunda rakipler bu işletmenin elindeki makineden daha verimli çalışan bir makine satın alacaktır. Dolayısıyla bu örnekteki işletmenin rekabet üstünlüğünü sürdürülebilir kılması için ürettiği makineyi geliştirmesi veya bir süre sonra eğer varsa kendi ürettiği makinenin daha verimli muadillerini satın alması beklenir.

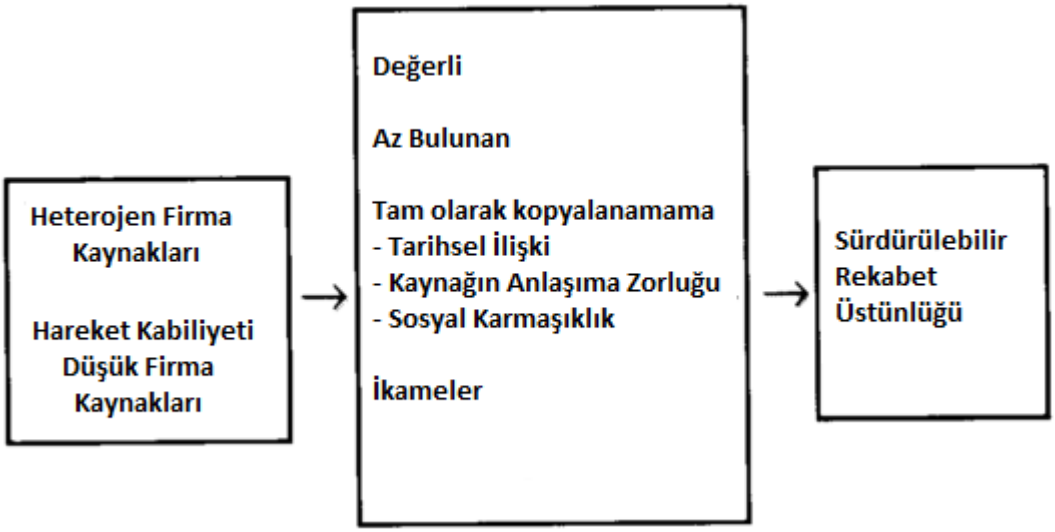
2.2.2. Sürdürülebilir Rekabet Üstünlüğü Sağlamada Kaynak Temelli Yaklaşım

Kaynak temelli yaklaşımın en önemli öncülerinden Barney'e göre bir işletmenin rekabet üstünlüğü sağlaması ancak ürettiği bir değer mevcut ve potansiyel rakipleri tarafından eş zamanlı olarak kopyalanamıyorsa sağlanır. Rakipler tarafından kopyalanmaya çalışılır ve bu başarılamazsa ve rakipler kopyalama girişimlerinden vazgeçerse rekabet üstünlüğü sağlayan bu özellik aynı zamanda sürdürülebilirdir **(Foss & Knudsen, 2000)**.

Sürdürülebilir rekabet üstünlüğü kavramı rekabet üstünlüğünün sonsuza kadar sürdürülebilir olmasıyla ilgili değildir. Sürdürülebilir rekabet üstünlüğü sağlayan bir değer, sektördeki ön görülemeyen bir değişimle beraber işletme için eski önemini

kaybedebilir dolayısıyla önceden olduğu gibi rekabet üstünlüğü sağlamayabilir. Dolayısıyla süründürülebilir rekabet üstünlüğü sağlamış bir işletme bu konumunu sektördeki büyük değişikliklerle yitirebilir. Ancak sektörde böyle bir değişim olmadığı bir durumda sürdürülebilir rekabet üstünlüğünün sadece rakiplerin kaynakları kopyalamasıyla kaybedilmesi mümkün değildir. Bir kaynağın başarılı bir şekilde kopyalanması o kaynağın sürdürülebilir rekabet üstünlüğü sağlamadığının ispatıdır.

Kaynak ve kabiliyetlerin rakipler tarafından hemen kopyalanamaması için sahip olmaları gereken bir takım özellikler de bulunmaktadır. Mesele öncelikle sektör bazında ele alınırsa kaynakların heterojen olması ve hareket kabiliyetlerinin düşük olması gerekir. Kaynakların homojen olarak dağıldığı yani tüm işletmelerin tüm kaynaklara eşit ölçüde ulaşabildiği bir sektörde geliştirilen stratejilerin rakipler tarafından kopyalanması çok kolay olacak dolayısıyla böyle bir ortamda sürdürülebilir rekabet üstünlüğünden de bahsetmek mümkün olmayacaktır **(Barney, 1991)**.



Şekil 4. Sürdürülebilir Rekabet Üstünlüğü ve Kaynaklar Arasındaki İlişki
Kaynak: (Barney, 1991)

Bir işletmedeki tüm kaynakların sürdürülebilir rekabet üstünlüğü sağlayamayacağı açıktır. Bir kaynağın bu potansiyele sahip olması için aşağıdaki özelliklere sahip olması gerekir **(Barney, 1991)**:

1. Kaynak değerli olmalı. Bir kaynağın değerli sayılması için kullanıldığı işletmenin verimliliğini arttırabilmeli. Klasik SWOT analizi yönteminde bir işletmenin başarısı o işletmenin fırsatları ne kadar iyi değerlendirdiğine ve tehditleri ne ölçüde bertaraf edebildiğine bağlanır. Bir kaynağın işletmenin verimliliğini arttırması yani değerli görülmesi de aynı şekilde işletmeye fırsat sağlaması veya bir tehdidi bertaraf etmesiyle ilgilidir.

2. Mevcut rekabet ortamında az bulunan bir kaynak olmalı. Bir kaynağın rakipler tarafından kolayca elde edilmesi o kaynağın sürdürülebilir rekabet üstünlüğü sağlamasını engeller. Bir kaynağın bol bulunması durumunda o kaynak çok değerli bir kaynak dahi olsa rekabet üstünlüğü sağamayacaktır. Hem değerli hem kolay bulunmayan kaynaklara sahip işletmeler genellikle teknolojik inovasyon gerçekleştirebilen firmalardır.

3. Sürdürülebilir rekabet üstünlüğü sağlayan kaynaklar değerli olmanın ve az bulunmanın yanında tam olarak kopyalanamama özelliğine de sahip olmalıdır. Bir kaynağın kopyalanamamasının değişik sebepleri olabilir. İlk sebep sürdürülebilir rekabet üstünlüğü sağlayan kaynağın elde edilmesindeki tarihsel avantaj olabilir. İkinci sebep bazı durumlarda rakiplerin sürdürülebilir rekabet üstünlüğü sağlayan kaynağı anlayamamalarıdır. Bazı durumlardaysa kaynak sahip olduğu sosyal kompleksite sebebiyle kopyalanamaz. Örneğin bir işletmenin müşterileriyle olan ilişkisini kopyalamak çok zordur **(Mugera, 2012)**.

4. Kaynağın değerli olan ama aynı zamanda da kolaylıkla bulunan veya eksiksiz olarak kopyalanabilecek bir ikamesi olmamalı. Böyle bir durumda rakipler değerli ve kolay bulunamayan bu kaynağı tam olarak kopyalamayı başaramasa bile ikamesini kopyalayabilir. Ya da ikame çok bulunan bir kaynaksa yine asıl kaynağın değerli oluşunun bir önemi kalmaz.

Dolayısıyla bir işletmenin sürdürülebilir rekabet üstünlüğü; değerli, az bulunur, tam olarak kopyalanamaz kaynaklara sahip olmasına ve bu kaynakların değerli bir ikamesinin olmamasına bağlıdır. Sürdürülebilir rekabet üstünlüğü sağlamış

işletmelerin sahip oldukları kaynaklar bu özelliklerini yitirirse, işletmeler temel yeteneklerini, dolayısı ile rekabet üstünlüklerini kaybederler.

3. Siber Saldırıların Firmaların Sürdürülebilir Rekabet Üstünlüğüne Etkisi

Kaynak temelli yaklaşım, işletmelerin rekabet üstünlüğü sağlamasındaki en önemli faktörü işletmenin kendine ait kaynakları olarak görürken endüstri temelli yaklaşım faaliyet gösterilen sektöre odaklanır. Ancak neticede endüstri temelli yaklaşım da işletmelerin sektördeki güçlerle başa çıkabilmesi için bir takım kaynak ve kabiliyetlere sahip olması gerektiğini kabul eder.

İşletmelerin sahip oldukları bu kaynaklar temelde üçe ayrılır: somut, soyut ve insan kaynakları. Somut kaynaklar işletmenin sahip olduğu ham madde, bina, arsa, makine, araç gibi gözle görülür kaynaklarken, soyut kaynaklar işletme bünyesindeki bilgi, birikim, örgütsel özellikler ve yetenekler, itibar ve patentler gibi kaynaklardır **(Özdemir & Denizel, 2006)**. İnsan kaynaklarıysa ikinci bölümde açıklandığı gibi işletme çalışanlarının bünyelerinde barındırdıkları bireysel değerlerdir.

Bu bölümde birinci ve ikinci bölümde oluşturulan çerçeve içerisinde siber casusluk ve siber sabotaj saldırılarının sürdürülebilir rekabet üstündeki etkisi endüstri ve kaynak temelli yaklaşım için incelenecektir.

3.1. Siber Casusluk Saldırılarının Sürdürülebilir Rekabet Üstünlüğüne Etkisi

Siber casusluk faaliyetleri siber uzayda bulunan verilerin çalınması durumudur. Burada gerçekleştirilen faaliyet, istisnai durumlar dışında fiziksel bir varlığın çalınmasını kapsamadan sadece bilişim sistemlerinde bulunan verinin çalınmasıyla ilgilidir. Dolayısıyla siber casusluk saldırılarının hedefi de işletmelerin soyut kaynaklarıdır.

Veri çalınması olayı fiziksel bir varlığın çalınmasından önemli bir farklılık gösterir. Fiziksel varlıklar çalındıktan sonra gerçek sahiplerine değil sadece onu çalana ait olurlar. Bu sebeple fiziksel bir varlığın çalındığı, çalındıktan sonra yerinde olmayacağı için kolaylıkla anlaşılabilir. Kimyasal bir ürünün formülü ya da iş süreçleri gibi soyut varlıklar çalındığındaysa bu varlıklar asıl sahiplerinde de

kalmaya devam eder. Bu yüzden de işletmelerin soyut kaynaklarını hedef alan siber casusluk saldırılarının tespiti çok zordur **(Lewis & Baker, 2013)**.

Diğer taraftan çalınan her veri rekabet üstünlüğüne aynı ölçüde zarar vermeyecektir. Bunun en büyük sebebi değişik kaynakların değişik seviyede kullanım kolaylığına sahip olmasıdır. Örneğin bir hammaddenin coğrafi keşif verisi rakipler tarafından kolaylıkla değerlendirilebilir. Fakat ileri teknoloji kullanan ve üretimi için yüksek maliyetli tesislere ihtiyaç olan bir makinenin planlarının kullanımı çok kolay olmayacaktır. Böyle bir bilginin kullanımı için bu bilgiyi ele geçiren firmanın yıllarını harcaması gerekebilir. Aynı şekilde bir iş sürecinin de rakip tarafından kullanılması bu tür kaynakların kopyalanmasındaki zorluklar nedeniyle tercih edilmeyebilir **(Mcafee, 2014)**.

3.1.1. Endüstri Temelli Yaklaşım Çerçevesinde Siber Casusluk

Endüstri temelli yaklaşımda işletmelerin bir sektörde rekabet üstünlüğü sağlaması, jenerik stratejilerden birini benimseyerek yani maliyet liderliği, farklılaştırma veya odaklanma stratejilerinden birini izleyerek sektördeki mevcut güçleri aşmasına bağlanır. Diğer bir değişle rekabet üstünlüğü sağlamış işletmeler jenerik stratejilerden birini başarıyla uygulamıştır. Rekabet üstünlüğünün sürdürülebilirliği ise sahip olunan rekabet üstünlüğünün uzun sürmesine bağlıdır **(Porter, 1998)**. Sonuç olarak rekabet üstünlüğünün kaybedilmemesi ve uzun sürmesi sahip olunan bu kaynakların varlığına bağlanabilir. Sürdürülebilir rekabet üstünlüğü sağlamak için önce rekabet üstünlüğü sağlamak gerektiği göz önünde bulundurulursa, rekabet üstünlüğü sağlayan kaynaklara yönelik saldırıların aynı zamanda sürdürülebilir rekabet üstünlüğüne yönelik olduğu da görülecektir.

Maliyet liderliği sağlayarak rekabet üstünlüğü sağlamak mal ve hizmet üretimi maliyetinin düşürülmesine bağlıdır. Çalışmanın ikinci bölümünde incelenen maliyet üstünlüğü sağlamada çoğunlukla kullanılan kaynaklar incelendiğinde bunların somut, soyut kaynaklar ve insan kaynaklarının kapsamında değerlendirilebileceği görülecektir. Siber casusluğun hedeflediği kaynaklarsa soyut kaynak olan; ürün planları, ar-ge sonuçları, formüller, ürün tasarımları gibi fikri mülkiyet kapsamına girecek kaynaklar ve bir ürün için yapılacak pazarlıkta teklif edilecek alt/üst fiyat limiti, kullanılan veya yatırım yapılacak hammaddelerin coğrafik bilgisi, kontrat

bilgileri, üretim süreci, ürünlerin müşteri listesi gibi ticari sır kapsamındaki kaynaklardır.

Bu kaynakların her birinin çalınması sektöre de bağlı olarak rekabet üstünlüğüne değişik ölçüde zararlar verecektir. Örneğin bir işletme ulaştığı ucuz hammadde sayesinde maliyet liderliği sağlamış olabilir. Eğer rakiplerin bu ucuz hammaddeyi kullanamamasının sebebi bu kaynağın varlığından bihaber olması veya nasıl ulaşacaklarını bilmemesiyse bu kaynakla ilgili siber ortamdaki veriler rekabet üstünlüğüne tesir edici özelliğe sahiptir. Veya verimli bir tesis kurularak maliyet liderliği sağlanmış ve bu tesisin verimli hale getirilmesinin altında ar-ge çalışmasıyla sahip olunmuş bir cihaz varsa bu cihazla ilgili her türlü veri de rekabet üstünlüğünü etkileyebilir. Bu cihazın planlarını ele geçiren rakipler rekabet üstünlüğü sağlamış işletmeninki kadar verimli tesisler kurarak rekabet üstünlüğünü ortadan kaldırabilir.

Farklılaştırma stratejisinin kurum içerisinde gerçekleştirilen ar-ge faaliyetleriyle ortaya konan bir değerle sağlanması mümkündür. Bu değer yeni bir teknoloji olabileceği gibi bir tasarım da olabilir. Örneğin ortaya koyduğu şık tasarımlarla müşterilerinin ilgisini çeken bir bilgisayar markasının siber ortamda bulunan tasarımları ürünleri piyasaya sürülmeden önce çalınıp kopyalanarak farklılaştırma stratejisine zarar verilebilir.

3.1.2. Kaynak Temelli Yaklaşım Çerçevesinde Siber Casusluk

Kaynak temelli yaklaşıma göre işletmeler ancak rakiplerinin hemen kopyalamayacağı türden kaynaklarla rekabet üstünlüğü sağlayabilir. Rakipler tarafından kaynakları kopyalama girişimleri gerçekleştirilmiş fakat başarılı olunamamış ve bu girişimlerden vazgeçilmişse rekabet üstünlüğü sürdürülebilir olarak nitelendirilir. Yani sürdürülebilir rekabet üstünlüğü sağlamış işletmeler, sektörü etkileyen makro ölçekli değişiklikler olmaması kaydıyla hiçbir şekilde rekabet üstünlüklerini kaybetmez ve kaynakları da kopyalanamaz **(Barney, 1991)**.

Kaynak temelli yaklaşımın sürdürülebilir rekabet üstünlüğü yaklaşımı göz önünde bulundurulduğunda siber casusluk yöntemiyle ele geçirilen bir bilgi (soyut kaynak) rakipler tarafından kopyalanabilmişse o kaynağın sürdürülebilir rekabet üstünlüğü sağladığı iddia edilemez. Sürdürülebilir rekabet üstünlüğü sağlayan bir bilgiyse siber

casusluk yoluyla ele geçirilse dahi rakip tarafından eksiksiz kopyalanamayacağı için etkisi sınırlı olacaktır.

İkinci bölümde ele alınan kaynak temelli yaklaşımın sağlanması için kullanılan kaynak türleri üçe ayrılmaktadır. Bunlardan ilki olan fiziksel kaynaklar, somut kaynaklar oldukları için siber casusluk yoluyla zaten ele geçirilemez. İkinci kaynak olan insan kaynaklarının da aynı şekilde siber casusluk saldırılarıyla doğrudan hedef seçilemeyeceğine değinildi. Ancak son kaynak çeşidi olan ve işletmedeki bireylerden oluşan grupların kendi içlerindeki ve işletme dışındaki insanlarla olan ilişkileriyle ilgili olan "örgütsel kaynaklar" siber casusluk yoluyla ele geçirilebilir. Ancak bu tip kaynaklar da rakipler tarafından bir şekilde öğrenilse dahi yapısal özellikleri sebebiyle uygulanması zordur. Örneğin müşteri ilişkilerini çok iyi yöneten ve bu yolla rekabet üstünlüğü sağlamış bir işletmenin bu özelliği e-posta yazışmalarını inceleyen siber saldırganlar tarafından tespit edilebilir. Fakat bu özellik tespit edilse dahi bunu kopyalamak oldukça zordur.

Sonuç olarak siber casusluk olayları kaynak temelli yaklaşım açısından ele alındığında sürdürülebilir rekabet üstünlüğüne fazla bir etkisinin olmayacağı söylenebilir.

3.2. Siber Sabotaj Saldırılarının Sürdürülebilir Rekabet Üstünlüğüne Etkisi

Siber sabotaj saldırıları çoğunlukla verilerin bütünlük ve erişilebilirliğini hedeflerken bazı durumlardaysa verinin gizliliğini ihlal ederek hedefe zarar verir. Bu çalışmanın ilk bölümünde verilen, siber saldırganların siber sabotaj yapma amaç ve yöntemleri incelendiğinde temelde kurumların üç kaynağının hedeflendiği görülmektedir: kurumdaki süreçlerin işleyişi, finansal kaynaklar ve itibar.

Siber sabotajda siber casusluk saldırılarının aksine işletmelerin soyut kaynaklarının yanında somut kaynakları da hedef alınabilir. Siber sabotaj aracılığıyla, örneğin somut bir kaynak olan bir makinenin işleyişi bozulabileceği gibi bir alışveriş sitesinin soyut kaynağı olan satın alma süreci de bozulabilir. Siber sabotaj saldırılarıyla işletmelerin çeşitli yöntemlerle finansal kaynakları hedeflenebilir ve ifşa edilmiş her saldırı işletmenin itibarına yönelik bir sabotaj özelliği gösterir.

Siber sabotaj saldırıları saldırıya uğrayan kuruma doğrudan zarar verdiği için tespit edilmesi de casusluk faaliyetlerine nazaran kolaydır. Ancak bazı durumlarda sabotajın hangi teknik yöntemle gerçekleştirildiğinin tespit zordur ki bu durum tespit edilen siber casusluk faaliyetleri dâhil tüm siber saldırılar için geçerlidir **(Marty, 2008)**.

3.2.1. Endüstri Temelli Yaklaşım Çerçevesinde Siber Sabotaj

Endüstri temelli yaklaşımda maliyet liderliği sağlamış işletmelerin sahip olduğu maliyet liderliği sağlayan kaynakları siber sabotaj saldırılarıyla verimsizleştirilebilir. Örneğin bir tesisin çalışması o tesisteki teknik mekanizmaların ayarlarıyla oynanarak veya doğrudan tesisin çalışması için gerekli disklerin silinmesiyle durdurulabilir. Ancak bu tip saldırıların etkisinin çok uzun sürmeyeceği de unutulmamalıdır.

Farklılaştırma stratejisini takip eden işletmelerse siber sabotaj saldırılarına karşı maliyet liderliği stratejisini takip edenlere göre daha savunmasızdır. Bunun sebebi farklılaştırma stratejisinin çoğunlukla itibar gerektirmesidir. Siber sabotaj yöntemiyle işleyişi bozulan bir sistem tekrar eski haline getirilebilir. Ancak özellikle ifşa olan saldırıların sebep olduğu itibar kaybının telafisi çok zor hatta özellikle güvenlik ve mahremiyetin kritik önemde olduğu bazı sektörlerde imkânsız olabilmektedir **(Schouwenberg, 2011)**.

Süreçleri veya itibarı hedef alan siber sabotaj saldırıları çoğunlukla finansal kaynaklara da dolaylı yoldan zarar verir. Örneğin bir alışveriş sitesine yapılan hizmet kesintisi saldırısı (DoS) sonucu o siteye erişim bir süre engellenirse o süre boyunca müşteriler alışveriş yapamayıp satın alma işlemlerini erteleyecek bazılarıysa rakip siteyi tercih edecektir. Siber saldırıların ifşası yoluyla borsa manipülasyonu da yine siber sabotaj saldırılarının başka bir finansal yan etkisidir. Siber saldırıya uğrayan işletmeler, bu durumun ifşası halinde %1 - %5 arasında değer kaybetmektedir **(Lewis J. A., 2013)**. Bunun dışında doğrudan finansal kaynakları hedef alan siber sabotaj saldırıları da yapılabilmektedir. Bu saldırılar, banka hesaplarındaki veya bitcoin cüzdanlarındaki paraların siber suçluların hesabına aktarımı şeklinde gerçekleşebildiği gibi fidye yazılımlarıyla da (ransomware) gerçekleşebilmektedir **(Bromium, 2014)**.

Maliyet liderliği stratejisi de farklılaştırma stratejisi de finansal kaynaklara ihtiyaç duyabilmektedir. Ama yine de finansal kaynakları hedef alan siber sabotaj saldırıları büyük ölçekli firmalara ciddi ölçüde zarar vermediği gibi, pek çok firma tarafından bu tip kayıplar siber uzayda faaliyet göstermenin bir maliyeti olarak görülür **(Bailard, Busony, & Lilienthal, 2013)**. Dolayısıyla finansal kaynakları hedefleyen siber sabotaj saldırıları daha çok orta ve küçük ölçekli işletmeleri etkilemektedir.

Sonuç olarak siber sabotaj saldırılarının maliyet liderliği stratejisi izleyen firmalar üzerindeki etkisinin sınırlı olduğu söylenebilir. Farklılaştırma stratejisini izleyen firmalarsa bu tip saldırılara karşı daha duyarlıdır.

3.2.2. Kaynak Temelli Yaklaşım Çerçevesinde Siber Sabotaj

Kaynak temelli yaklaşımda rekabet üstünlüğü de, sürdürülebilir rekabet üstünlüğü de kaynakların kopyalanamamasına bağlıdır. Siber sabotaj saldırılarıysa kaynakları kopyalama girişimleriyle değil kaynakların kullanılamaz hale getirilmesi veya verimsizleştirilmesiyle ilgilidir. Yani siber sabotaj saldırısı sonucunda rekabet üstünlüğü sağlayan kaynakların zarar görmesi söz konusudur.

Siber sabotaj saldırılarıyla işletmelerin yazılımları, üretimde kullanılan makineler gibi "fiziksel kaynakları" zarar görebilir. Bu saldırıların itibar üzerindeki veya iş süreçleri üzerindeki etkisi işletmenin müşterileriyle olan ilişkilerine zarar verebileceği için "örgütsel kaynaklar" da bu tip saldırılardan etkilenebilir. İnsan kaynaklarıysa siber sabotaj saldırılarına karşı diğer iki kaynak türüne göre daha dirençlidir. Dolayısıyla kaynak temelli yaklaşıma göre sürdürülebilir rekabet üstünlüğü siber sabotaj saldırından etkilenebilir.

Tablo 2. Siber Casusluk ve Siber Sabotajın Sürdürülebilir Rekabet Üstünlüğüne Etkisi

Sürdürülebilir Rekabet Üstünlüğü Yaklaşımı		**Siber Casusluk**	**Siber Sabotaj**
Endüstri Temelli Yaklaşım	Maliyet Liderliği	Etkili	Sınırlı Etki
	Farklılaştırma	Etkili	Etkili
Kaynak Temelli Yaklaşım		Sınırlı Etki	Etkili

4. Konunun Uygulamadaki İzdüşümü

Başarılı bir siber saldırıya maruz kalmış olan işletmeler itibar kaybının önüne geçmek için bu saldırıların gizlenmesini tercih ederler. Yapılan araştırmalar borsada işlem gören firmaların saldırı sonrasında değerinin %1 ile %5 arasında düştüğünü göstermektedir **(Lewis & Baker, 2013)**. İşletmelerin kendilerini hedefleyen başarılı siber saldırıları paylaşma konusundaki isteksizlikleri bu alanda yapılan çalışmaları da sınırlandırmaktadır.

İfşa edilen saldırılar incelendiğinde bunların büyük bir kısmının siber sabotaj saldırıları olduğu ve saldırganlar tarafından kendi reklamlarını yapmak ve saldırdıkları işletmenin itibarına zarar vermek için ifşa edildiği görülecektir. Amacı gereği gizli gerçekleştirilen siber casusluk saldırılarınınsa tespiti daha zordur. Tespit edilse dahi saldırganların ele geçirdiği bilgiyi ve bunu hangi amaçla kullandığını kesin olarak bilmek çoğu zaman mümkün değildir.

Bu bölümde siber saldırı olayları siber casusluk ve siber sabotaj başlıkları altında işlenerek bunların işletmelerin hangi kaynaklarını hedeflediği ve ne sonuç alındığı incelenecektir.

4.1. Siber Casusluk Saldırıları Olaylarının İncelemesi

4.1.1. Lockheed Martin Siber Casusluk Olayı

Siber saldırganlar 2011 yılında, RSA isimli ABD merkezli siber güvenlik firmasına e-posta yoluyla içerisinde zararlı kod bulunan bir Excel dosyası gönderdi. Bu dosyanın açılmasıyla firmanın sistemlerine giren saldırganlar firmanın SecurID sistemine ulaşmayı başardı **(Fidelis, 2011)**. SecurID sistemi uluslararası boyutta hizmet veren bir firma olan RSA'in çeşitli sistemlere iki boyutlu yetkilendirmeyle erişim sağlanması için ürettiği bir teknolojidir ve pek çok kurum tarafından kullanılmaktadır.

ABD savunma sanayisinin bel kemiği konumunda olan Lockheed Martin de SecurID sistemi üzerinden kendi sistemlerine dışarıdan erişim yapılmasını sağlamaktaydı. Siber saldırganlar RSA'in SecurID sistemi üzerinden Lockheed Martin'in

sistemlerine de sızarak pek çok ar-ge çalışmasını çaldılar. Bu çalışmalar arasında içinde Türkiye'nin de bulunduğu dokuz ülkenin geliştirilmesinde yer aldığı F-35 savaş uçağı da bulunmaktadır **(Schwartz, 2011)**.

2014 yılında Çin vatandaşı ve bir havacılık firmasının da sahibi olan Su Bin, Kanada tarafından bu saldırıyı gerçekleştirdiği için tutuklandı. Su Bin bu saldırıyı yine Çin vatandaşı olan iki kişiyle birlikte gerçekleştirdiğini de itiraf etmiştir. Ayrıca Su Bin ele geçirdiği verileri Çin devletine de satmıştır **(Walker, 2014)**.

Saldırı, Su Bin'in kendi havacılık firmasına başka bir firmanın ar-ge çalışmalarını siber casusluk yoluyla transferi gibi gözükmektedir. Ancak diğer taraftan Çin'in, ABD Başkanı Barack Obama'nın 2014 yılında Çin'e gerçekleştirmiş olduğu ziyaret sırasında ilk olarak ortaya çıkardığı J-31 ve J-21 savaş uçaklarının F-35'in sahip olduğu bazı parçalara sahip olduğu da iddia edilmektedir **(Wee, 2015)**. Sonuç olarak saldırının kaynağı kesin olarak bilinmemekle birlikte amacının ar-ge çalışmalarını çalmak olduğu açıktır.

4.1.2. Nortel İflası

Nortel bir dönem Kanada'nın en büyük firması konumunda bulunan ve telekomünikasyon alanında faaliyet göstermiş uluslararası ölçekli bir firmadır. Firma 2009 yılında iflasını açıklayıp sahip olduğu tüm varlıkları Avaya, Ciena, Telefon AB L.M. Ericsson ve Genband gibi firmalara satmıştır **(Gorman, 2012)**.

Firmanın 19 yıllık siber güvenlik danışmanı Brian Shields, 2012 yılında CBC'deki "As It Happens" isimli programda vermiş olduğu mülakatta firmanın iflasının sebebinin Çin kaynaklı siber casusluk operasyonları olduğunu açıklamıştır. Buna göre 2012 yılında iflas eden firmadaki siber casusluk saldırısı en az 2000 yılına uzanmakta ve firmanın iflasına kadar sürmektedir **(CBC News, 2012)**.

Öncelikle Nortel'in CEO'su dâhil firmada çalışan yedi kişinin sistemlere giriş için kullandıkları hesaplar, siber saldırganlar tarafından ele geçirilmiştir. Bu hesaplarla firma içerisinde geliştirilen yazılım kodlarından, pazarlama çalışmalarına kadar pek çok konuda verinin yer aldığı ana dosya sistemlerine ulaşım sağlanmıştır. Siber

saldırganlar bununla da yetinmeyip ihtiyaç duydukları yerlerde bazı bilgisayarlara zararlı yazılım bulaştırarak bunlar üzerinden de veri çalmıştır **(Gorman, 2012)**.

1988 yılında kurulan Çin Telekomünikasyon firması Huawei'nin yükselişi de tam olarak Nortel'in düşüşüne denk gelmektedir. Shields, Çin tarafından Nortel'den çalınan ticari sır ve fikri mülkiyet kapsamındaki bilgilerin Huawei'ye verilerek rekabet üstünlüğü sağlandığını iddia etmektedir. Bu olay hem ar-ge çalışmalarının hem de iş planlarının çalınması sonucu bir firmanın ne derece büyük zarar görebileceğinin önemli bir örneğidir **(Chaffin, 2012)**.

4.2. Siber Sabotaj Saldırıları Olaylarının İncelemesi

4.2.1. Saudi Aramco Disklerinin Silinmesi

Saudi Aramco Suudi Arabistan merkezli petrol ve doğal gaz şirketidir. Dünyanın en büyük petrol rezervine sahip olan şirket aynı zamanda dünyanın en büyük petrol ve doğalgaz firmasıdır **(Forbes, 2015)**.

Firmaya 2012 yılında gönderilen ve içinde zararlı yazılım barındıran bir e-postanın çalışanlar tarafından açılmasıyla birlikte yazılım kendini hızla şirket içindeki diğer bilgisayarlara da kopyalamaya başlamıştır. Shamoon ismi verilen zararlı yazılım yayıldığı bilgisayarların disklerindeki verileri geri döndürülemez şekilde silmiştir.

Şirket ağı içinde hızla yayılan yazılımı durdurmak için teknik bir yöntem bulamayan Aramco çalışanları, çareyi dünyadaki tüm ofislerindeki tüm bilgisayarların network kablosunu çıkarmakta bulmuştur. Bu süre zarfında zararlı yazılım 30000 ile 55000 arasında bilgisayarı etkilemiştir. On gün boyunca network kabloları takılmayan ve internet erişimi olmayan bilgisayarlar nedeniyle firmanın günlük pek çok işi kesintiye uğramıştır. Telefonların dahi kullanılamadığı bu süreçte, dünyanın en büyük petrol ve doğalgaz şirketinin çalışanları daktilo gibi eski teknolojileri kullanarak işlerini devam ettirmeye çalışmıştır. Firma Suudi Arabistan içindeki petrol satışlarını durdurmuş ancak on yedi gün sonra petrolü ücretsiz vermek zorunda kalmıştır **(Pagliery, 2015)**.

Bu süreçte firma sorunu çözmek için dünyanın çeşitli yerlerinden pek çok siber güvenlik uzmanından destek almıştır. Bununla birlikte hard disk üretimi yapan uzak

doğudaki fabrikalardan doğrudan ve çok yüksek fiyatlarla 50 bin hard disk satın almak zorunda kalmıştır **(UK Ministry of Defence, 2013)**.

Saldırı "Cutting Sword of Justice" isimli siber aktivist grup tarafından üstlenmiş ve saldırıyı Suud ailesinin otoriter yönetimine tepki amacıyla gerçekleştirdiklerini açıklamışlardır **(Cutting Sword of Justice, 2012)**. Bununla birlikte saldırının kısa süre önce İsrail merkezli büyük bir siber saldırıya maruz kalan İran tarafından gerçekleştirildiği de iddia edilmektedir.

Bu saldırı, siber sabotaj saldırısı yoluyla Aramco içindeki iş süreçlerinin bozulmasına ve büyük maddi kayıplara yol açmıştır. Aramco'da bu süreçte görev yapmış olan siber güvenlik uzmanı Christina Kubecka'ya göre bu saldırı Aramco'dan daha küçük ölçekli bir firmanın iflasına yol açabilirdi **(Rashid, 2015)**.

4.2.2. Sahte Diginotar Sertifikası Üretilmesi

Diginotar, Vasco Data Security isimli Hollanda firmasın dijital sertifika otoritesidir. Başka firmaların da ürettiği dijital sertifikalar sayesinde kullanıcılar, sertifikaları kullanan web sitelerine girdiklerinde hatlarının dinlenmesi ve bilgilerinin ele geçirilmesi engellenmektedir. Diginotar tarafından üretilmiş sertifikalar; CIA, MI6, Mossad, Microsoft, Yahoo, Skype, Facebook, Twitter, Microsoft ve daha pek çok kurum tarafından kullanılmıştır **(Greene, 2011)**. Dolayısıyla Diginotar itibarın çok önemli olduğu bir sektörde hizmet vermiştir.

1 Temmuz 2011 yılında Diginotar'ın web sunucularından birinde bulunan bir güvenlik zafiyeti sayesinde saldırganlar, Diginotar sistemine giriş yapmayı başarmıştır. Sistem içerisine girdikten sonra sertifika sunucularına ulaşan saldırganlar sahte sertifikalar üretmeyi başarmıştır. Üretilen sahte sertifikalar arasında google.com da bulunmaktadır ve bu sertifikalarla 298.140 adet farklı IP sahte e-posta web sitelerine yönlendirilerek kullanıcıların bilgileri çalınmıştır. Saldırıya maruz kalan kullanıcıların büyük kısmının İran vatandaşı olması sebebiyle saldırının İran tarafından gerçekleştirildiği kanaati yaygındır **(Espiner, 2012)**.

Saldırı Diginotar tarafından tespit edildikten sonra iki ay boyunca gizlenmiş ve bu süre zarfında sahte sertifikalar nedeniyle pek çok kullanıcı mağdur olmuştur. Saldırı

ifşa olduktan sonraysa Diginotar'ın sertifikaları kurumlar tarafından kara listeye alınmıştır. Sonuç olarak 20 Eylül 2011'de Vasco, Diginotar'ın iflasını ilan etmek zorunda kalmıştır **(Vasco, 2011)**.

Diginotar saldırısı hem siber sabotaj hem de siber casusluk saldırılarıyla ortaklıklar taşımaktadır. Saldırının amacı aslında insanların bilgisini çalmaktır ama bunun için kullanılan yöntem Diginotar sunucularındaki verilerin bütünlüğünü bozmaktır. Dahası saldırı ifşa olmuş ve firmanın itibarına karşı çok büyük etkisi olmuş sonunda firma iflasa sürüklenmiştir.

4.2.3. Associated Press Twitter Hesabı Saldırısı

Associated Press'in Twitter hesabını ele geçiren Suriye Elektronik Ordusu isimli Suriye rejimi tarafından desteklenen bir grup, 23 Nisan 2013 tarihinde bu hesap üzerinden bir tweet attı. İki milyon takipçisi olan Associated Press'in twitter hesabından atılan tweete göre Beyaz Saray'da iki patlama olmuş ve Barack Obama yaralanmıştı.

Şekil 5. AP'nin Twitter Hesabından Verilen Haber
Kaynak: (Smith, 2013)

Atılan bu tweetten sonra paniğe kapılan insanlar Dow Jones borsasından paralarını hızla çekmeye başladı. Beyaz Saray basın sözcüsü Jay Carney bu tweet karşısında basına Obama'nın iyi olduğu yönünde açıklama yapmak zorunda kaldı. Ama Carney,

buna rağmen borsanın atılan bir tweet sebebiyle 100 milyar dolar kaybetmesini engelleyememiştir **(Curtis, 2014)**.

Associated Press'in maruz kaldığı bu siber sabotaj saldırısıyla büyük çaplı finansal zarara yol açılmıştır. Bu saldırı, siber sabotaj yöntemleriyle borsa manipülasyonunun mümkün olduğunu da göstermektedir.

SONUÇ

Küreselleşen piyasa şartlarının da zorlamasıyla stratejik yönetim içerisinde rekabet üstünlüğü ve rekabet üstünlüğünün sürdürülebilirliği meseleleri önemini arttırmıştır. Rekabet üstünlüğü genel olarak, Porter'ın başını çektiği endüstri temelli ve Barney'nin öncülerinden olduğu kaynak temelli, iki farklı yaklaşımla incelenmektedir. Rekabet üstünlüğünün sürdürülebilirliği Porter tarafından zamana bağlanırken Barney ise tarafından kaynakların rakipler tarafından kopyalanamamazlığıyla açıklanmıştır.

Bilişim teknolojilerinin hayatın her alanında sürekli daha fazla yer kapladığı günümüzde iş dünyası da bu teknolojileri kullanmak zorundadır. Özellikle büyük ölçekli firmaların iş süreçlerinin işlemesi için gerekli olan temel bileşen haline gelen bilişim teknolojileri pek çok zafiyet te barındırmaktadır. Bu sistemlerde bulunan verinin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanamadığı durumlarda işletmeler önemli ve değişik türde zararlar görebilmektedir.

Siber uzayda bulunan bu verilerin gizliliğinin ihlal edildiği bazı durumlar siber casusluk olarak nitelendirilirken, gizlilik, bütünlük ve erişilebilirliğinin ihlal edildiği durumlarsa siber sabotaj olarak kabul edilmiştir. Bu iki yöntemin kullanılmasıyla çeşitli derecelerde devlet bağlantısı olan (veya hiç olmayan) siber saldırganlar, iş dünyasını da hedef alabilmektedir. Haksız şekilde rekabet üstünlüğü sağlamayı amaçlayan bu saldırıların sürdürülebilir rekabet üstünlüğü sağlamış işletmelerin bu durumlarının değiştirilmesi konusunda da etkisi bulunabilmektedir.

Siber casusluk çalışmaları çoğunlukla daha komplike saldırılar olduğu için özellikle kendi ülkelerindeki kritik sektörlere fayda sağlamayı amaçlayan devletler tarafından tercih edilmektedir. Porter'a göre rekabet üstünlüğü sağlamak için maliyet liderliği veya farklılaştırma stratejilerinden birisi izlenmelidir. Bu stratejilerin uygulanmasıysa bir takım kaynak ve kabiliyetlerin varlığına bağlıdır.

Porter'ın savunduğu sürdürülebilir rekabet üstünlüğü kavramı incelendiğinde rekabet üstünlüğü kaynaklarına siber casusluk yöntemleriyle zarar verilebileceği görülecektir. Örneğin bir işletmedeki haftalar alan bir iş süreci o firma tarafından geliştirilmiş bir yazılımla günler içerisinde yapılabiliyorsa bu yazılım maliyet liderliği aracılığıyla rekabet üstünlüğü sağlayabilen bir kaynak olarak görülebilir. Ancak bu yazılım bir siber casusluk yöntemiyle rakip firma tarafından ele geçirildiğinde artık rekabet üstünlüğü kaynağı olarak görülemez.

Barney'e göreyse rekabet üstünlüğü hemen kopyalanamayan kaynaklara bağlıdır. Eğer bir işletmenin rekabet üstünlüğü kaynakları, rakipleri tarafından kopyalanmaya çalışmış ama bunda başarılı olunamamışsa ve rakipler kopyalama girişimlerinden de vazgeçmişse bu firmanın rekabet üstünlüğünün sürdürülebilir olduğu söylenebilir. Barney sürdürülebilir rekabet üstünlüğü konusunda kopyalanamamayı ön plana

alırken siber casusluksa verilerin kopyalanması ve kullanılmasıyla ilgilidir. Dolayısıyla Barney'nin kaynak temelli yaklaşımına göre siber casusluk saldırıları sürdürülebilir rekabet üstünlüğü üzerinde önemli bir etkiye sahip değildir.

Siber sabotaj saldırılarının gerçekleştirilmesi çoğunlukla siber casusluk saldırılarına göre daha kolaydır. Bu saldırıları genellikle devletlerle doğrudan irtibatı olmayan siber saldırganlar tercih eder. Kurumların siber ortamda bulundurduğu verilerin bütünlüğünü bozmayı, erişilebilirliğini engellemeyi ve verileri ifşa ederek gizliliğini ortadan kaldırmayı amaçlayan bu saldırılar işletmelere oldukça büyük zararlar verebilmektedir.

Porter'ın endüstri temelli yaklaşımı çerçevesinde siber sabotaj saldırıları, siber casusluk saldırılarında olduğu gibi sürdürülebilir rekabet üstünlüğüne zarar verebilir. Müşterilerinin gözünde sahip olduğu itibar ve güvenilirlik sayesinde rakiplerinden farklılaşmış ve rekabet üstünlüğü sağlamış bir işletme, müşteri bilgilerinin siber saldırganlar tarafından ifşa edilmesiyle bu üstünlüğünü yitirebilir.

Barney'nin kaynak temelli yaklaşımı çerçevesinde de siber sabotaj saldırıları "örgütsel kaynaklar" üzerinde etkili olabilmektedir. Bu yaklaşım için özellikle iş süreçlerinin bozulmasına sebep olan siber sabotaj saldırıları oldukça etkilidir.

Sonuç olarak siber saldırılar; sürdürülebilir rekabet üstünlüğü üzerinde Porter'ın endüstri temelli bakış açısıyla etkiliyken, Barney'nin kaynak temelli bakış açısına göre siber sabotaj saldırıları önemli etkiye sahipken siber casusluk saldırılarının etkisi sınırlıdır.

KAYNAKLAR

AlAli, A. (2015). *Anonymous | from inception to corruption*. 12 21, 2015 tarihinde cyberkov.com: https://blog.cyberkov.com/2711.html adresinden alındı

Amir, W. (2015, Aralık 15). *11 Ongoing anonymous operations you must know about*. 12 21, 2015 tarihinde hackread.com: https://www.hackread.com/11-anonymous-operation-you-should-know/ adresinden alındı

Andress, J., ve Winterfeld, S. (2013). *Cyber warfare, second edition: techniques, tactics and tools for security practitioners.* Syngress.

Andrew Jones, G. L. (2015). *Global information warfare: the new digital battlefield.* Auerbach Publications.

Avusturya. (2013). *Austrian cybersSecurity strategy.* Vienna: Federal Chancellery of the Republic of Austria.

Bailard, F., Busony, B., ve Lilienthal, G. (2013). Organized cyber crime and bank account takeovers. Federal Reserve Bank of San Francisco.

Barca, M. (2009). Stratejik yönetim düşüncesinin evrimi. *Ankara Sanayi Odası Bülteni*.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*.

Boxall, P. (1998). Achieving competitive advantage through human resource strategy: towards a theory of industry dynamics. *Human Resources Management Review, 3*.

Bromium. (2014). *Understanding crypto-ransomware.* Bromium.

Bryant-Kutcher, L., Jones, D. A., ve Widener, S. K. (2008). Market valuation of intangible resources: The use of strategic human capital. M. Epstein, & M. A. Malina içinde, *Book Series: Advances in Management Accounting.* Emerald Group Publishing Limited.

CBC News. (2012, Şubat 16). *Nortel collapse linked to chinese hackers*. 12 12, 2015 tarihinde CBC: http://www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591 adresinden alındı

Chaffin, L. (2012, Ekim 7). *60 Minutes torpedoes huawei in less than 15 minutes*. 12 12, 2012 tarihinde networkworld: http://www.networkworld.com/article/2223272/cisco-subnet/60-minutes-torpedoes-huawei-in-less-than-15-minutes.html adresinden alındı

Cornish, P., Livingstone, D., Clemente, D., ve Yorke, C. (2010). *On cyber warfare a chatham house report.* Londra: Chatham House.

Curtis, S. (2014, Haziran 13). *Syrian electronic army hacks microsoft twitter accounts*. 12 12, 2012 tarihinde telegraph: http://www.telegraph.co.uk/technology/internet-security/10568019/Syrian-Electronic-Army-hacks-Microsoft-Twitter-accounts.html adresinden alındı

Cutting Sword of Justice. (2012, Ağustos 15). *pastebin*. 12 12, 2012 tarihinde pastebin: http://pastebin.com/HqAgaQRj adresinden alındı

Das, T. K., ve Teng, B.-S. (2000). A resource-based theory of strategic alliances. *Journal of Management*.

Drab, D. (2003). *Economic espionage and trade secret theft: defending against the pickpockets of the new millennium.* XEROX.

Ekizer, A. (2014, Ocak 15). *TCK'da bilişim suçları*. 12 12, 2015 tarihinde ekizer.net: http://www.ekizer.net/tckda-bilisim-suclari/ adresinden alındı

Espiner, T. (2012, Kasım 2). *DigiNotar hack details revealed by dutch government*. 12 12, 2012 tarihinde scmagazineuk: http://www.scmagazineuk.com/diginotar-hack-details-revealed-by-dutch-government/article/266739/ adresinden alındı

Fidelis. (2011, Eylül 9). *Fidelis threat advisory #1001 the rsa hack.* 12 15, 2015 tarihinde fidelissecurity: https://www.fidelissecurity.com/sites/default/files/FTA1001-The_RSA_Hack.pdf adresinden alındı

forbes. (2015). *The world's 25 biggest oil companies*. 12 12, 2015 tarihinde forbes: http://www.forbes.com/pictures/mef45ggld/1-saudi-aramco-12-5-million-barrels-per-day/ adresinden alındı

Foss, N. J., ve Knudsen, T. (2000). The resource-based tangle: towards a sustainable explanation of competitive advantage. Institut for Industriøkonomi og Virksomhedsstrategi.

Geers, K. (2011). *Strategic cyber security.* Tallinn: CCD COE Publication.

Germany Federal Ministry of the Interior. (2011). *Cyber security strategy for germany.* Berlin: Federal Ministry of the Interior.

Gorman, S. (2012, Şubat 13). *Chinese hackers suspected in long-term nortel breach*. 12 12, 2015 tarihinde The Wall Street Journal: http://www.wsj.com/articles/SB10001424052970203363504577187502201577054 adresinden alındı

Göral, R. (2009). Sürdürülebilir rekabet üstünlüğü sağlamak için stratejik teknoloji yönetimi ve otomotiv yan sanayi firmaları üzerine bir araştırma. Selçuk Üniversitesi.

Grant, R. M. (1991). The resource-based theory of competitive advantage: implication for strategy formulation. *California*.

Greathouse, C. B. (2014). Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? Kremer, Jan-Frederik, Müller, & Benedikt içinde, *Cyberspace and International Relations.* Springer.

Greene, T. (2011, Eylül 20). *DigiNotar certificate authority goes bankrupt*. 12 12, 2012 tarihinde networkworld: http://www.networkworld.com/article/2181294/security/diginotar-certificate-authority-goes-bankrupt.html adresinden alındı

Hacking Team. (2015). *hackingteam*. 12 21, 2015 tarihinde hackingteam: http://www.hackingteam.it/ adresinden alındı

Hopia, H. (2015). *Dawn of the Drones: Europe's Security Response to the Cyber Age.* Wilfried Martens Centre for Europians Studies .

Klimburg, A. (2012). *National Cyber Security Framework Manual.* Tallinn: NATO CCD COE.

Leiner, B. M. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review, 39*(5).

Lewis, J. A. (2013). *Conflict and Negotiation in Cyberspace.* Center for Strategic and International Studies.

Lewis, J. A., ve Baker, S. (2013). *The Economic Impact of Cybercrime and Cyber Espionage.* McAfee.

López, J. E., Salazar, E. A., Castro, G. M., ve Sáez, P. L. (2006). Organizational capital as competitive advantage of the firm. *Journal of Intellectual Capital, 3*.

Lord, M., ve Sharp, T. (2011). *AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE.*

Lorenz, B., ve Kikkas, K. (2012). Socially Engineered Commoners as Cyber Warriors – Estonian Future or Present ? *Cyber Conflict (CYCON), 2012 4th International Conference on.*

Ludewig, O., ve Sadowski, D. (2009). Measuring Organizational Capital. O. Ludewig, ve D. Sadowski içinde, *Organizational Capital.*

Macaskill, E., ve Dance, G. (tarih yok). *NSA FILES: DECODED Waht the revelations mean for you*. 12 26, 26.12.2015 tarihinde theguradian: http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 adresinden alındı

Marty, R. (2008). *Applied security visualization.* Boston: Pearson Education.

Mcafee. (2014). *Net Losses: Estimating the Global Cost of Cybercrime.* Center for Strategic and International Studies.

McGraw, G., ve Fick, N. (2011). Separating Threat from the Hype: What Washington needs to know about Cyber Security. G. McGraw, ve N. Fick içinde, *What Washington Needs to Know About Cyber Security.* Center for a New American Security (CNAS).

McGraw, G., ve Fick, N. (2011). SEPARATING THREAT FROM THE HYPE: WHAT WASHINGTON NEEDS TO KNOW ABOUT CYBER SECURITY. K. M. Lord, ve T. Sharp içinde, *America's Cyber Future.*

Minarik, M. (2007). Cost Leadership & Differentiation - An investigation of the fundamental trade-off between Porter's cost leadership and differentiation strategies. Stockholm School of Economics Institute of International Business.

Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. *Informing Strategies and Developing Options for U.S. Policy.* National Research Council of the National Academies.

Mugera, A. W. (2012). Sustained Competitive Advantage in Agribusiness: Applying the Resource-Based Theory to Human Resources. *International Food and Agribusiness Management Review, 4*.

Özdemir, Ö., ve Denizel, M. (2006). A resource based and context dependent model of firm competitiveness. *POMS 2006 17th Annual Conference Proceedings.*

Pagliery, J. (2015, Ağustos 5). *The inside story of the biggest hack in history*. 12 12, 2012 tarihinde CNN: http://money.cnn.com/2015/08/05/technology/aramco-hack/ adresinden alındı

Porter, M. E. (1998). *Competitive strategy: Techniques for analyzing industries and companies.* New York: The Free Press.

Rashid, F. Y. (2015, 8 8). *Inside The Aftermath Of The Saudi Aramco Breach*. 12 12, 2012 tarihinde darkreading: http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676 adresinden alındı

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law.* Oxford Scholarship.

Savage, K., Coogan, P., ve Lau, H. (2015). *The evolution of ransomware.* Symantec.

Schouwenberg, R. (2011). Diginotar: Cyber war, CAs and the death of online trust. Boston: Kaspersky Lab.

Schwartz, M. J. (2011, 5 30). *Lockheed Martin Suffers Massive Cyberattack*. 12 12, 2015 tarihinde darkreading: http://www.darkreading.com/risk-management/lockheed-martin-suffers-massive-cyberattack/d/d-id/1098013? adresinden alındı

Seviçin, A. (2009). "Sürdürülebilir Rekabet Üstünlüğü" Kavramı Üzerine Bir İnceleme. *ZKÜ Sosyal Bilimler Dergisi, 5*(10).

Sigholm, J. (2013). non-state actors in cyberspace operations. *Journal of Military Studies, 4*(1).

Smith, G. (2013, 4 23). *Syrian Electronic Army's AP Hack Just The Latest Phishing Attack On A Major News Organization*. 12 12, 2012 tarihinde huffingtonpost: http://www.huffingtonpost.com/2013/04/23/syrian-electronic-army-ap-twitter-hack_n_3140849.html adresinden alındı

Soyer, A. (2007). Organizasonlar İçin Rekabet Üstünlüğü Modeli Oluşturulması ve Rekabet Üstünlüğü Kaynaklarının Analizi. İstanbul Teknik Üniversitesi.

T.C. Başbakanlık. (2008). *Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı.* 12 27, 2015 tarihinde tbmm.gov.tr: http://www2.tbmm.gov.tr/d24/1/1-0483.pdf adresinden alındı

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.* T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı.

Theohary, C. A., ve Rollins, J. W. (2015). *Cyberwarfare and Cyberterrorism: In Brief.* Congressional Research Service.

Tim Maurer, R. M. (2014). *Compilation of Existing Cybersecurity and Information Security Related Definitions.* New America.

UK Cabinet Office. (2011). *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.* Londra: UK Cabinet Office.

UK Ministry of Defence. (2013). *Joint Doctrine Publication (JDP) Cyber Primer.*

Ulsch, M. (2014). *Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks.* Wiley.

United Kingdom Houses of Parliment Parliamentary Office of Science & Technology. (2011). *Cyber Security in the UK.* United Kingdom, Parliamentary Office of Science & Technology, POSTnote Number 389: Cyber Security in the UK, 2011, p. 1.

USA Today. (2015, Ocak 5). *Timeline: North Korea and the Sony Pictures hack*. 11 10, 2015 tarihinde USA Today: http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/ adresinden alındı

Ülgen, H., ve Mirze, K. (2013). *İşletmelerde Stratejik Yönetim.* Beta.

Vasco. (2011, Eylül 20). *VASCO Announces Bankruptcy Filing by DigiNotar B.V.* 12 12, 2012 tarihinde Vasco: https://www.vasco.com/company/about_vasco/press_room/news_archive/2011/news_vasco_announces_bankruptcy_filing_by_diginotar_bv.aspx adresinden alındı

Walker, D. (2014, temmuz 14). *Chinese man charged with hack of Boeing, Lockheed Martin aircraft data*. 12 12, 2015 tarihinde scmagazine:

http://www.scmagazine.com/chinese-man-charged-with-hack-of-boeing-lockheed-martin-aircraft-data/article/360786/ adresinden alındı

Wee, S.-L. (2015, haziran 19). *China calls Snowden's stealth jet hack accusations "groundless"*. 12 12, 2015 tarihinde reuters: http://www.reuters.com/article/usa-china-cybersecurity-idUSL4N0UY31Y20150119 adresinden alındı

Yiğit, S., ve Özyer, K. (2011). Sürdürülebilir Rekabet Üstünlüğü Kaynağı Olarak Bilgi. *SÜ İİBF Sosyal ve Ekonomik Araştırmalar Dergisi*(21).

Zhou, M. (2005). Network Intrusion Detection: Monitoring, Simulation and Visualization.

ÖZGEÇMİŞ

Adı Soyadı : Yavuz Atlas

Doğum Yeri ve Yılı : İstanbul, 1986

Medeni Hali : Bekar

Yabancı Dili : İngilizce

E-posta : yavuzatlas@gmail.com

Eğitim Durumu

Lise : Şişli Anadolu Lisesi, 2004

Lisans : İstanbul Kültür Üniversitesi, Fen Edebiyat Fakültesi, Matematik-Bilgisayar Bölümü, 2010

Yüksek Lisans : Coventry University,
Mühendislik Departmanı, Yazılım Geliştirme Bölümü, 2014

Mesleki Deneyim

İstanbul Ticaret Üniversitesi, Bilgi İşlem Daire Başkanlığı	2011-2012
TÜBİTAK BİLGEM, Siber Güvenlik Enstitüsü	2011-2012
Biznet Bilişim, Güvenlik Testleri Birimi	2014-…(devam ediyor)