T.C. İSTANBUL TİCARET ÜNİVERSİTESİ

DIŞ TİCARET ENSTİTÜSÜ

WORKING PAPER SERIES

Tartışma Metinleri

WPS NO/ 45/ 2016-06

E-TİCARET VE SİBER İŞLEMLER

Duygu VAROĞLU ŞİMŞEK*

Oktay ÇINAR**

* duygu.vr@gmail.com, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Muhasebe Denetim Tezli Yüksek Lisans Programı Öğrencisi

** oktay.cinar@hotmail.com.tr, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Muhasebe Denetim Tezli Yüksek Lisans Programı Öğrencisi

E-TİCARET VE SİBER İŞLEMLER

ÖZET

Bilgi çağının gerekliliklerine uygun olarak kitle iletişim araçlarının çeşitlenmesinin yanında, hemen hemen her tür talebimizin karşılandığı televizyon ve internet dünyası, tüm ekonomik işlemlerin yapıldığı platformlar haline gelmiştir. Küreselleşmenin kaçınılmaz sonucu olarak tüm kitle iletişim araçları buna hizmet etmektedir. İnternet ve televizyon üzerinden yapılan satışlar da doğal olarak parabolik şekilde artmaktadır. İnsanların çoğunlukla zamanını geçirdiği bu sanal ortamlar bazı güvenlik sorunlarını da yanında getirmektedir. Sadece sosyal ve ticari amaçlarla değil, aynı zamanda eksikliklerine bağlı olarak suç unsurlarını da beraberinde getirmektedir. Öyle ki; 24.03.2016 tarihli "Kişisel Verilerin Korunması Hakkında Kanun'un" yürürlüğe girmesinden sadece 1 hafta sonra nüfusumuzun yarısından fazla kişinin kişisel verileri "kimin tarafından ele geçirilip yayınlandığı hala belli bile değilken" internet ortamında yayınlanmıştır.

Anahtar kelimeler; Elektronik Ticaret, Bilgi Çağı, Küreselleşme, Güvenlik

ABSTRACT

As well as the diversification of the mass communication tools, television and internet technologies became the main platforms that we spend most of our time and use for the economic transactions. As a result of globalization, all mass communication tools are serving in this manner. Naturally, there's a parabolic increase in sales through internet and television. These virtual places that people spend most of their time would bring some security problems with them. Not only social and commercial wise, but also criminal factors would be formed according to the deficiencies of this age. So that; just after one week that the "Personal Data Protection Law" published on 24th of March 2016, the identity information of the half of total our population has been declared on internet even we have no idea who is the responsible.

Key words; Electronic Trade, Information Age, Globalization, Security

Giriş

Günümüz dünyası artık dijital dünya haline gelmiştir. Bunun en önemli nedeni de küresel ekonomik hareketlerin sundukları ve bilişim çağının gerekliliklerdir. Artık teknoloji toplumsal hayatın ayrılmaz bir parçasını oluşturmaktadır. Genel olarak geçmişe ya da alışkanlıklarına sıkı sıkıya bağlı olan insan önemli icat ve fikirleri benimsemede tutucu davranmış olsa da bilgi işlem alanındaki değişikliklere ani ve hızlı tepkiler verip benimsemiştir. Teknolojik yeniliklerin beşiği olan askeri birimler tarafından genellikle savunma amacıyla icat edilen internet; 1960' lı yılların başında kullanılmaya başlanmış ve toplumların kullanımına sunulmuştur.

Başlangıçta şifreleme ve şifre çözme amacıyla ortaya çıkan bilgisayarlar Rusya ve ABD gibi ülkelerin gizli savaşlarının bir ürünü olarak gelişimini hızlandırmış ve bugünkü noktalara kadar gelmesine sebep olmuştur.

Bilişim teknolojilerinde yaşanan gelişmeler bireyler kadar uluslararası toplumun da ilgisini çekmekte ve derinden etkilemektedir. Özellikle bilgisayarlar kullanılarak oluşturulan araçlar ve yöntemler, gerçek dünyanın yanında bir de "siber dünya" meydana getirmiştir. Siber alan kişi ve toplumlara da uluslararası bir siber kimlik sahibi olmasına neden olmuş dolayısıyla da siber bir dünya ve siber kimlikler siber yapılar ortaya çıkarmış yaşadığımız dünyanın yanında ayrı sınırlar ve sonuçlar doğurmuştur. Bu siber dünya bireylerin ve toplumların günlük yaşamlarında çok önemli faydalar ve kolaylıklar da sağlamaya başlamış olsa da kötü niyetli ve bilinçsiz kullanımdan dolayı bazı dezavantajları da beraberinde getirmiştir. Bu doğrultuda karşılaşılan sonuçlar bilgi çağının bedeli olarak görülebilse de gerçek hayatta karşılaşılan suç, kabahat ve sorunları da aynı zamanda sanal ortama ya da siber alana taşımış oldu. Siber alanda suç ve suç unsurlarının bilgi çağının gerekliliği nedeniyle sürekli dönüşmesi bu suç unsurlarına karşı önlemlerin alınmasını da zorlaştırmaktadır. Çoğu zaman da yönetimleri çözümsüz ve çaresiz bırakmaktadır.

Günümüz şartları insanları, toplumları ve ülkeleri elektronik dünyanın bir parçası haline getirmiştir. Bu değişime ayak uyduramayan kişi toplum ve devletler çağın gerisinde kalmaya mahkûmdur.

1. TAKASTAN E-TİCARETE

2.1. Elektronik Ticaret Kavramı ve Kısa Tarihi

İnternet bilgi, eğlence iletişim ve elektronik ticaret amacıyla kullanılabilir. Elektronik Ticaret Koordinasyon Kurulu'na göre elektronik ticaret; Kişiler ve kurumların; açık ağ (bağlantı) çevresinde (internet) ya da belirli sayıda kişi tarafından erişilebilen kapalı ağ ortamlarında (intranet) yazı, ses ve görüntü şeklindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanan ve bir değer yaratmayı amaçlayan ticari işlemlerinin tümünü ifade etmektedir (Elektronik Ticaret Koordinasyon Kurulu, 2016). Dünya Ticaret Örgütü'nün tanımına göre de elektronik ticaret; Mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılmasıdır (WTO, 2016).

İhtiyaçlar insanlıkla birlikte var olmuştur. İhtiyaçlar insanları sürekli bir arayış içerisine sokmuş ihtiyaçlar karşılandıkça yeni ihtiyaçlar doğmuştur. İhtiyaçların temininin zorluğu insanları birbirleriyle etkileşim dairesine almış ve birbirlerinden ihtiyaçlarını karşılıklı olarak temin edecekleri basit ve ilkel pazarların oluştuğu takas ekonomisinin doğmasına neden olmuştur. Takas ekonomisi ile birlikte nüfusun da artması, temel ihtiyaçların dahi karşılanamamasına neden olmuştur. Çünkü sadece artan ihtiyaçlar değil ihtiyacı olana ulaşabileceği kanallara da ihtiyaç duyulmuş ve hem ihtiyaçlar şekillenmiş hem de farklı yöntemler doğmuştur. İnsanların ihtiyaçlarının peşinde olması günümüze kadar gelen ekonomi akımlarının doğmasına, Sanayi Devrimi gibi kırılma noktalarına, sömürgelerin yapılmasına dolayısıyla da ülkeler arasında savaşların da temel dinamiği olmuştur.

İnsanlığın değişmesi ve gelişmesi beraberinde bir bütün olarak dünyayı da dönüştürmüştür. Özellikle son 20 yılın ekonomik devrimi olan küreselleşmeyle birlikte sınırların ortadan kalkması, matbaanın icadından günümüz iletişim kanallarının artması ve çeşitlenmesi Dünya'yı tamamen bir "küresel bir köy" haline getirmiştir (Marshall, 2015: 37). Küreselleşme aynı zamanda yer küre üzerindeki tüm insanları hedef almış ve mevcut kimliklerinin de dışında yeni bir "küresel kimlik" oluşturmuştur. Bu küresel kimliğin geçerliği de tamamen ekonomik bir meta haline gelmiş insana koyduğu kurallara uymak zorunda bırakmıştır. Öyle bir noktaya getirmiştir ki insanı, parasını vererek tükettiği bir ürün henüz tükenmeden yine aynı insanı hedef alarak aynı ürünün yeni bir sürümünü tüketmeye zorlamıştır ve de çoğunlukla da başarılı olmuştur. İnsan nüfusunun artmasından daha büyük artmaktadır ekonomik parametrelerin büyümesi. Ekonomik göstergelerin yazılı olarak büyümesi insanlığın aynı oranda geliştiğini ya da zenginleştiği anlamına asla gelmez. Çünkü

zengin daha zengin fakir daha fakir olarak yoksulluk, açlık ve buna bağlı hastalıklarda da belirgin düzeyde artış olmaktadır.

Dünya Ticaret Örgütünün 2015 verilerine göre (WTO, 2016); dünyanın en zengin 61 kişisinin servetinin toplamı Dünya nüfusunun yarısının servetine eşittir. Aynı şekilde dünya nın en zengin % 1 lik nüfusu, geri kalan nüfusun toplamının zenginliğine eşit durumdadır.

Günümüzde 2015 yılı için dünya ticaret hacmi yıllık 19 trilyon dolar seviyelerine ulaşmıştır (TİM, 2015). Oysa 1980'lerde bu rakam 2,03 trilyon dolardır. Aynı zamanda dünya e-ticaret hacmi de 2015 yılı itibariyle 1,5 trilyon dolara yaklaşmıştır (WTO, 2016).

İletişim alanında, içinde bulunduğumuz 20. yy. içerisinde, teknolojideki yeni buluşların da etkisiyle akıl almaz boyutta ilerlemeler kaydedilmiştir. Her şeyi sorarak bulan insan, bilgiyi muhafaza edecek yer aramıştır ve muhafaza edeceği bilgi arttıkça da başka arayışlara geçmiş ve elektronik ortamda saklama fikri doğmuştur. Elektronik ortamda, bilginin daha az alan kapladığı ve bu bilgiye erişimin daha basit olduğu görülmüştür. Odalara sığmayan büyük bilgi kaynakları artık mikroçiplere sığmaktadır.

İletişim ve bilgi teknolojilerindeki gelişmelere bağlı olarak 1985'li yıllarda ikinci yarısında ortaya çıkmış olan "elektronik ticaret" kavramıyla ilk defa www.amazon.com adlı web sitesinde ilk kitap satılmasıyla karşılaşıyoruz. Bu satışın arkasından aynı yıl içerisinde e-mail (elektronik posta) yoluyla pazarlama ve reklam keşfedilmiştir.

ARPA projesiyle başlayan girişimler sonucu 1980'lerde Amerikan NSF (National Science Faundation-Ulusal Bilim Vakfı) beş tane süper bilgisayar merkezi kurmuştur. Bu merkezleri sadece savaş üreticisi firmalar ve dev araştırma firmaları kullanmaktaydı. Bu merkezleri bağlamak için ARPAnet'in teknolojisi kullanılmıştır. ARPANET (Gelişmiş Araştırma Projeleri Dairesi Ağı), Birleşik Devletler Savunma Bakanlığı bünyesine bağlı ARPA (Gelişmiş Savunma Araştırmaları Projeleri Birimi) tarafından geliştirilen dünyanın ilk paket dağıtımı ağı ve evrensel internetin öncülüdür.

1993 yılında Beyaz Saray (White House), online/çevrimiçi olarak internete bağlanmıştır. 1994 yılında, Web üzerinde işlem yapmayı sağlayan Mosaic yazılımı piyasaya sürülmüş ve kullanım kolaylığı nedeniyle çok yaygınlaşmıştır. Ayrıca Amazon.com'da ilk alıcılarının karşısına çıkmış ve satılmış; e-mail yoluyla pazarlama ve reklam keşfedilmiştir. 1995 yılında ise internet üzerinde işlem yapan Netscape yazılımı aktif bir şekilde kullanıma gelmiştir (Uysal ve Tunç, 1996: 7).

Aynı yıl "Yahoo!" Adlı arama motorunda ilk arama yapılmış; e-Bay'da ilk sanal müzayede düzenlenmiştir (NTV MAG Dergisi, 2001:87).

Aramanın yapılıyor olması sizi hedef gören firmaları eğer aradığınız ürünü sunuyorlarsa aradığınız anda sizi yönlendirecek şekilde karşınıza çıkabilmektedirler. İnsanları yaptıkları aramaya göre yönlendirme şansını sağlamıştır. Elektronik ticaret firmaları bu araştırmalarınızın sonucu olarak karşınıza reklam vs. ile çıkabilmektedirler dolayısıyla e-ticaret üzerinden reklam sektörünün de doğması ve büyümesi sonucunu doğurmuştur.

İnternet bilgi, eğlence iletişim ve elektronik ticaret amacıyla kullanılabilir. Elektronik ticaret; insanların ve kurumların; açık ağ ortamında (internet) ya da sınırlı sayıda kullanıcı tarafından ulaşılabilen kapalı ağ ortamlarında (intranet) yazı, ses ve görüntü şeklindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanan ve bir değer yaratmayı amaçlayan ticari işlemlerinin tümünü ifade etmektedir (Elektronik Ticaret Koordinasyon Kurulu, 2016).

Dünya Ticaret Örgütü nün tanımına göre de elektronik ticaret Mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılmasıdır (WTO, 2016).

1.2. Elektronik Ticaretin Kapsamı, Araçları ve Faydaları

Elektronik araç ve açık ve kapalı elektronik ağları üzerinden, üretim, tanıtım ve her türlü ticari ilişkinin yapılması ve her türlü ödemenin yapılması ile ilgili faaliyetlerin tümünü kapsamaktadır. Her türlü mali, sınai, nakdi ya da fikri hakkın alınıp satıldığı, kiralandığı bir alandır.

Elektronik ticaret; bilgisayar üzerinden internet, faks (belgegeçer), sabit ya da mobil telefon ve elektronik veri transferi araçlarıyla yapılabilmektedir. Yani tüm kitle iletişim araçları elektronik ticaretin olmazsa olmaz araçlarıdır.

Elektronik ticaretin hem müşteri/tüketici hem de üretici ya da satıcı açısından faydaları bulunmaktadır. Müşteri açısından talep ettiği ürünü temin etme, karşılaştırma, daha ucuza tedarik etme yani maliyet azaltımı gibi temel faydaları bulunmaktadır. Tüketici veya satıcılar açısından ise, stok maliyetinin azalması, aracıların aradan çıkarılarak kar oranının artması ve etkili görsel reklam yöntemlerinden yararlanma gibi faydalar elde edebilmektedir. Artan elektronik ticaret hacmi nedeniyle daha büyük kitlelere daha ucuz ve hızlı bir şekilde ulaşma kabiliyeti kazandırma gibi faydaları göz ardı edilemeyecek düzeydedir.

Dünya'nın genel ekonomik göstergelerinde yatay ve negatif seyre rağmen elektronik ticaretin hacminin artmasının bazı temel nedenleri şunlardır;

- Nüfusun artması
- Ödeme sistemlerinin gelişmesi

- Bilgisayar, akıllı telefon kullanımının artması
- Internet kullanımının yaygınlaşması
- Elektronik reklam harcamalarının ve yöntemlerinin çeşitlenmesi
- Elektronik ticarete karşı olan ön yargıların değişmesi
- Güvenlik tedbirlerinin artması ve yasal düzenlemelerin yapılmasıdır.

1.3. Elektronik Ticaretin Geldiği Nokta; "Son Nokta"

Türkiye gelişmekte olan ülkeler arasında sayılır yıllardır. Her ne kadar genç bir nüfusa sahip olmak faydalı sayılsa da yeniliklere uyum sürecinin kısalması gibi gelişmekte olan hatta az gelişmiş ülkelerin bazı karakteristik özelliklerini de belirgin bir şekilde taşımaktayız. İnternet abonesi sayısının 19 milyon olduğu ülkemiz 2015 Yılında yaklaşık 43 milyon internet kullanıcısına (Dijitalajanslar, 2016) sahip olarak şu anki durumuyla Avrupa'nın 6.büyük internet popülasyonuna sahip. Tabi bu gelişmişlik göstergesi olarak görülse de az gelişmiş ve gelişmekte olan ülkelerin lüks mallara olan talep esnekliğinin yüksek olmasından da kaynaklanabilmektedir. Dünya ölçeğinde ise bu rakam yaklaşık 3 milyar kişi civarındadır (Dijitalajanslar, 2016).

Stratejik olarak ve coğrafi olarak kritik bir konumda bulunan ülkemiz bunun doğal sonucu olarak lojistik ve bankacılığın da gelişmiş olması 2 önemli unsura dikkat çekmektedir. Alışverişe olan tutkumuz ve bu tutkunun gücü olan kredi kartları kullanım düzeyimiz. Bankalararası Kart Merkezi'nin (BKM) son paylaştığı rakamlar kredi kartı sayımız yaklaşık 58 milyon, banka kartı sayımız ise 82 milyona ulaşmış durumdadır. Toplam rakam 140 milyon civarında olup toplam nüfusun neredeyse 2 katıdır (İktisadi, 2016).

Ülkemiz de elektronik ticarette en çok kredi kartı kullanılsa da birçok ülke de farklı ödeme yöntemleri öne çıkmaktadır. Örneğin Romanya'da kapıda ödeme yöntemi, Polonya' da ise EFT / Havale yöntemi daha yaygın kullanılmaktadır. Güney Afrika da ise mobil ödeme yöntemi kullanılmaktadır (İTO, 2016).

2015 yılı itibariyle Türkiye e-ticaret pazarında 27 milyar TL hacim sağladı. Söz konusu dönemde gerçekleştirilen işlem sayısı ise yaklaşık 148 milyon iken Türk insanı kişi başı ortalama 229 TL değerinde elektronik ticaret hacmi olmuştur. Dünyada ise durum aynı doğrultudadır. Dünya genelinde elektronik ticaret hacmi 2015 yılında 19 trilyon dolar seviyelerine gelmiştir. Ancak bu büyüme rakamlarının en fantastik olanını gerçekleştiren ülke Çin' dir. Çin tek başına yaklaşık 3 trilyon dolar seviyelerinde elektronik ticaret hacmine ulaşmış durumdadır (E-Ticaret, 2016).

2. SİBER ALANDA GERÇEK GÜVEN

Elektronik ticaret en büyük problemi güvenliktir. Elektronik pazarlarda tüketici, alıcı ya da hedef kitle ile sağlıklı, uzun süreli ve etkili bir iletişim kurabilmenin en önemli yolu "güven alanı" nı sağlamaktır. Bu güven alanını siber alanda sağlamak pek de kolay bir iş değildir. Güven alanını sağlamanın en önemli anahtarı güven olgusunu anlayabilmektir.

Elektronik ortamda ticaret hacminin arttırılmasından ziyade elektronik ticaretin güvenliğinin sağlanması gerekmektedir. Herkes tarafında erişilebilir olması, kişisel verilerin algoritmik formüllerle korunarak kötü niyetli 3. kişilerin eline geçmesinin engellenmesi, satıcı ile alıcı arasında geri bildirim ortamının oluşturulması, satış sonrası hizmet sağlanarak tüketicinin çekincelerinin bertaraf edilmesi gerekmektedir. Siber alanda güvenlik tesis etmenin önündeki en önemli sorun özgürlük ile güvenlik faktörünün dengelenmesidir. Güven sağlanırken, güveniyor olmak kişisel bilgilerinin paylaşılabileceği söz konusu asla olmamalıdır. Siber ortamda yapılan alışverişin yasal dayanakları çok önemsenmese de dikkat edilmesi gerekmektedir, gerekli yasal düzenlemelerin varlığı ve detaylı olarak bilgi güvenliğini sağlayıcı önlemler alınmış olması gerekir. Ayrıca mesafeli satış sözleşmelerine dikkat edilip, satıcının tabiiyeti hatta bulunduğu ülkenin yasal düzenlemelerinin bilemeyeceğimizden kişisel veri paylaşımında uluslararası önlemlerin alındığına dikkat edilmesi gerekmektedir. Tüketici ilişkileri ticaretinin temeli açık bir şekilde müşteri sadakatine bağlıdır. Sadık ve sürekli alım yapan kişilerin işletmenin kendi hayatını sürdürmesinin ve gelirlerinin garantisidir. Alıcı ve satıcı arasındaki güven davranışının farklı özellikleri olsa da güven unsuru ortaktır (Sahay, 2003:556).

Alıcı-satıcı arasındaki güven ilişkisi ekonomik bir anlama da sahiptir. Başka bir ifadeyle alıcı-satıcı arasında maliyet-fayda faktörü etkilidir. Alıcı ve satıcı arasında ilişkinin devam etmesi için maliyet ve fayda dikkate alınır. Eğer tüketicinin bu alışverişten elde edeceği fayda, katlanması gereken maliyetten daha yüksek ise satıcı ile olan alışveriş devam edecektir. Tersi durumda, tüketici tercihlerini değiştirecektir. Güven dürtüsü öncelikle öngörü süreciyle belirlenir. Alıcı ve satıcı alışverişe konu olan taraflardır. Taraflar karşı tarafın davranışlarını öngörmeye çalışır. Güvenilirliğini test etmeye çalışır. Öngörü ile gerçekleşen arasındaki farkın en az olabilmesi için karşı tarafın geçmişteki hareketlerinden haberdar olması gerekir. Taraflar eğer tam bilgiye sahip olup aynı zamanda basiretli bir iş adamı gibi (Türk Ticaret Kanunu, 2016) davranıyorlarsa birbirlerine güven tesis edilmiş olacaktır. Herhangi bir mal ve hizmet alışverişi durumunda tahmin/öngörü ile sonuç arasındaki farkın seviyesinin düşüklüğü taraflar arasında güven unsurunun temelini oluşturacaktır (McCole, 2002:82).

Risk öngörüsü güven ölçütüdür de. Eğer risk öngörüsü yüksekse güven tesis etmek her iki taraf için de imkansıza yakındır. Tutum, kişilerin veri bir obje hakkında olumlu veya olumsuz öğrenilmiş davranış potansiyelidir (Wibowo ve Japarianto, 2013:6).Tutum, ticari hayatın önemli unsurlarından biridir. Çünkü özellikle alıcı tarafın kararını tutumu belirler (Solomon, Bamossy ve Askegaard, 2002:132).

Eğer alıcıların bir ürüne ya da satıcıya karşı olumlu bir tutum içerisindelerse onları almaya ikna etmek daha kolay olacak ve alışveriş gerçekleşecektir. Aksi halde yani ürüne ya da satıcıya karşı olumsuz bir tutum içerisindelerse ikna etmek imkansız ya da imkansıza yakın olacaktır. Bu durumda olumsuz algı ya da tutumu olumlu ya çevirmek pazarlamacılar ve satıcılar arasından zor ve maliyetli bir durumdur. Negatif ya da nötr durumu pozitife çevirmek de pazarlamacının görevidir (Fisher, 2003).

3.1.Siber Güvenliğin Düşman Askerleri

Elektronik ticaretin hacmi, kullanım kolaylığı, kişisel verilerin elde edilmesinin önemi kötü niyetli 3. Kişilerin iştahını kabartmakta olup saldırı yöntemlerinin de çok çeşitli tehdit unsurlarının varlığına neden olmuştur. Alınan önlemlerin yetersizliğinin yanında bilinçsiz bir kullanıcının tuzaklara çok kolay yakalanabilmesi siber tehdit alanının ne denli korkunç bir saha olduğunu önümüze sermektedir. Siber sahada karşılaşılan sorun ve tehditler sanal ortamın sınırsızlığı içerisinde bir sınırlandırmaya gidilmesi pek mümkün bir durum değildir. Her alanda çok yönlü tehditler sunmaktadır. Bu nedenle siber güvenliğin aslında ne kadar önemli bir sorun olduğunun bir göstergesi durumundadır.

Genel olarak bilgi vermek üzere; siber saldırıların başlıca tehdit araçları ve yöntemleri arasında (Ünver ve Canbay, 2010:598) ;

- casus yazılımlar (spyware),
- aldatma (IP spoofing),
- servis dışı bırakma (DoS),
- yemlemeler (phishing)
- istem dışı elektronik postalar (spam),
- klavye işlemlerini kaydeden programlar (key loggers),
- virüsler,
- Truva atları,
- kurtçuklar (worms),
- zombie
- botnet,

- şebeke trafiğinin dinlenmesi (sniffers),
- propaganda

olarak çeşitleri sıralayabiliriz.

3.2. Gerçek Saldırı ve Siber Güvenlik

Bilişim teknolojilerinde yaşanan gelişmeler gerçek dünyanın yanında ve bütünleyici bir parçası olarak "siber alan" ortaya çıkmıştır. Yanında birçok fayda ve avantajın yanında zarar ve dezavantajlar da getirmiştir. Yaşanan hızlı gelişmelere ayak uyduramayan özelikle de gelişmemiş, az gelişmiş ve gelişmekte olan ülkelerde yönetimleri tehditlere karşı önlem alma karşı koyma ve engelleyebilme konusunda yetersiz bırakmıştır. Bu durumda yönetimler yapabilecekleri fazla bir seçenek olmadığından geleneksel yöntemlere başvurarak yasaklama ve erişim engelleme yöntemlerini seçmektedirler. Buna karşılık gelişmiş ülkeler; olası siber tehditlere karşı hem tehdidi önleyici tedbirler hem de savunmayı güçlendirici "siber kuvvetler" oluşturmaya başlamışlardır.

Siber sahadaki işlemlerin kolay ve izi silinebilir yapılabiliyor olması devletler düzeyinde de ilgi çekmiş ve özellikle soğuk savaş dönemlerinde ve hala başvurulan bir yöntem olarak görülmektedir. Bu açıdan baktığımızda ileriki dönemlerde "siber savaş" ların yaşanabileceği ve tüm Dünya' da "gerçek etkiler" doğurabileceğini söyleyebiliriz. Çünkü özellikle gelişmiş ülkelerin savunma sistemleri ileri düzey bilgi sistemleri kullanılarak oluşturulduğu, yönetildiğini göz önünde tutarsak gelişmiş ülkeler siber saldırı tehdidi altındadır diyebiliriz. Örneğin Çin şu anda önemli siber saldırı kapasitesine ve gelişmiş istihbarat alt yapısına sahip bir devlet olarak 2050 yılına kadar elektronik egemenliği hedefleyen ve düşman kuvvetlerinin altyapılarını etkisiz hale getirebilmeyi de içeren bir "siber doktrin" benimsemiştir (United States-China Economic and Security Review Commission, 2008).

4. İdeal Bir Siber Saldırı Sahası Olarak; Türkiye

Türkiye; yukarıda bahsettiğimiz üzere; oldukça fazladır, yaklaşık 43 milyon internet kullanıcısına (Tuik, 2016a) sahip olarak şu anki durumuyla Avrupa'nın 6.büyük internet popülasyonuna sahip Dünyanın en büyük 18. Ekonomisi durumundaki Türkiye (halbuki IMF verilerine göre 30 yıl önce, 1976 yılında G20 ye 17. Sıradan girmiş (Academia, 2016), gelişmekte olan bir ülke deyip neredeyse yarım asırdır gelişimini tamamlayamamış bir ülke olarak) nedense tüketim verilerine baktığımızda her daim sıralamada ilk 10 görmek olası bir durum ve maalesef "dövünülecekken övünülesi bir halet-i ruhiyeye girmeye her daim namzet bir ülke" konumundadır.

Ülke olarak genelde “kervan yolda düzelir .” atasözüne layık olarak; teknolojiyi üretmek bir yana dursun teknolojiyi satın alma konusunda öncü olmuştur. Gelişmişlik ve her alanda zenginlik düzeyi; bilgi çağında teknoloji üretebilen ve ihraç edebilen ülkelerin tasarrufundadır. Toplum olarak en düşük gelir düzeyindeki kişilerde bile akıllı telefon kullanım oranının yüksekliğine düşük eğitim ve bilinç seviyesi ile yüksek kredi kartı kullanımı ve tüketime/ tüketmeye aşık bir toplum profili her zaman siber saldırı açısından cazip bir seviyeye çıkarmaktadır ülkemizi. Çünkü yüksek oranda ama bilinçsiz kredi kartı kullanımı oranı düşük güvenlik ve kolay suç işleme sonucunu doğurmaktadır. Nitekim aşağıdaki tablo1’de de görüleceği üzere (EGM, 2016); kredi kartı ve sahteciliği suçlarının artışındaki belirgin artış göze çarpmaktadır.

Tablo 1: 2003-2012 Yıllar Arası Siber Suç Sayıları

Sucun Nevi Ve Yıllara Göre Olay Sayıları	*Kredi Kartı Sahteciliği ve Dolandırıcılığı*	*Banka Dolandırıcılığı*	*Bilişim Suçları ve Dolandırıcılığı*	*İnternet Aracılığıyla Dolandırıcılık*	*Diğer*	*Toplam*
Olay Sayısı 2003	*80*	*15*	*X*	*X*	*X*	*95*
Olay Sayısı 2004	*146*	*22*	*16*	*X*	*X*	*184*
Olay Sayısı 2005	*195*	*9*	*91*	*X*	*X*	*295*
Olay Sayısı 2006	*122*	*98*	*4*	*X*	*X*	*224*
Olay Sayısı 2007	*594*	*642*	*416*	*X*	*91*	*1.743*
Olay Sayısı 2008	*830*	*1.177*	*560*	*X*	*157*	*2.742*
Olay Sayısı 2009	*1.511*	*550*	*353*	*412*	*45*	*2.871*
Olay Sayısı 2010	*1.131*	*151*	*972*	*71*	*28*	*2.353*
Olay Sayısı 2011	*1.772*	*141*	*1.738*	*111*	*31*	*3.793*
Olay Sayısı 2012	*1.724*	*264*	*3.669*	*278*	*783*	*6.718*

Kaynak: https://www.cyber-warrior.org (Erişim Tarihi: 21 Nisan 2016)

Türkiye’de bilinen ilk siber suç 1990 yılında karşılaşılan banka kartı dolandırıcılığıdır. Bu dönemlerde davaların sayısal olarak az olmasının nedeni; dava sayılarındaki düşüklüğün sebebi; kanunda yerinin ve tanımının olmaması aynı zamanda da siber suçlarla mücadele edecek önleyici güvenlik donanımına sahip olunmamasıdır. Okur yazar seviyesinin düşüklüğü, yasal hakkını arama basiretini gösterememe ve bilgisayar gibi teknolojik argümanları kullanma oranının düşüklüğünden kaynaklanmaktadır (İlbaş ve Köksal,1990-2011). Son yıllarda siber suçlar ile ilgili artışın olduğu gözlemlenmektedir. Bunun nedeni olarak, bilişim ürünlerinin kullanım oranlarının hiperbolik olarak artması, elektronik ticaretin günden güne yaygınlaşmasını örnek verebiliriz.

Tablo 2: 2003-2012 Yıllar Arası İşlenen Siber Suçlarda Yakalanan Şüpheliler

Sucun Nevi Ve Yıllara Göre Olay Şüpheli Sayıları	*Kredi Kartı sahteciliği ve Dolandırıcılığı*	*Banka Dolandırıcılığı*	*Bilişim Suçları ve Dolandırıcılığı*	*İnternet Aracılığıyla Dolandırıcılık*	*Diğer*	*Toplam*
Olay Sayısı 2003	*268*	*49*	*X*	*X*	*X*	*317*
Olay Sayısı 2004	*422*	*72*	*31*	*X*	*X*	*525*
Olay Sayısı 2005	*543*	*33*	*179*	*X*	*X*	*755*
Olay Sayısı 2006	*241*	*172*	*9*	*X*	*X*	*422*
Olay Sayısı 2007	*907*	*1.187*	*764*	*X*	*134*	*2.992*
Olay Sayısı 2008	*991*	*2.114*	*842*	*X*	*416*	*4.363*
Olay Sayısı 2009	*2.176*	*1.113*	*534*	*731*	*116*	*4.670*
Olay Sayısı 2010	*1.005*	*300*	*1.346*	*115*	*134*	*2.900*
Olay Sayısı 2011	*1.429*	*327*	*1.842*	*283*	*123*	*4.004*
Olay Sayısı 2012	*630*	*120*	*1.085*	*289*	*289*	*2.180*

Kaynak: TÜİK

Tablo 1 ve 2 dikkate alındığında , 2007 yılı sonrasında işlenen siber suçlar ve ilgili şüpheliler artmaktadır. Bunun nedeni olarak siber suçlarla ilgili savunma birimlerinin oluşması ve etkin çalışması sayılabilir.

Siber suçların sayısının belirgin olarak az olmasında; hem teknolojinin yaygınlaşmasındaki ağırlık hem de ki en önemlisi ceza kanunlarında yerinin olmamasından kaynaklanmaktadır. Çünkü suç olarak tanımlanmayan bir fiile nasıl ceza verebilirsiniz? Önce kanunda tanımlanması gerekir ki ceza verebilesiniz. Tanımlanmış olsa bile tanımının dar olması maalesef etkin sonuçlar doğmasına izin vermeyecektir. Öyle ki; Siber suçlar ülkemiz mevzuatına 1991 yılı Türk Ceza Kanunu'nda (TCK), eklenen "Bilişim Alanında Suçlar" bölümüyle yer bulmuştur. 2004 yılında çıkarılan 52373 sayılı yeni TCK'da siber suçlar, siber suçlar sahasının iyice gelişmesiyle ve halen de gelişmekte olmasıyla daha ayrıntılı biçimde yer almıştır. 5237 sayılı yeni TCK'da bilişim alanında suçlar (Resmi Gazete, 2016);

- *Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu (m.243),*
- *Bilişim sisteminin isleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu (m.244/1-2),*
- *Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (m.244/4),*
- *Banka veya kredi kartlarının kötüye kullanılması suçu (m.138),*

Aynı zamanda özel hayata ve hayatın gizli alanına karsı suçlar bölümündeki siber suçları;

- *Kişisel verilerin kaydedilmesi (m.135),*
- *Kişisel verileri hukuka aykırı olarak verme veya ele geçirme (m.136),*
- *Verilerin yok edilmemesi suçları (m.138),*
- *bilişim sistemleriyle işlenebilecek diğer suçlar; 91. md.*

olarak belirlenmiştir. Bunu yanı sıra 5070 sayılı "Elektronik İmza Kanunu" da güvenlikli elektronik işlem yapmayı güvence altına almayı amaçlamaktadır.

4.1.Siber Güvenlik Önlemleri ve Türkiye Vatandaşlarının Verilerinin Sızma Sorunsalı

Siber güvenlik alanı gelişmekte olan ve gelişimini tamamlamamış bir alandır. Bu konuda ülkemiz güvenlik birimlerinin kabiliyetleri, tedbir argümanları ve nitelikli elaman ve nitelikli ekipman sayısı yetersizdir (Cyber-warrior,2016).Bu yetersizliğe siber alanda karşılaşılan suçlara karşı müdahalenin uluslararası boyutu da eklenince yapılması gereken hala çok şeyin olduğunu görebilmekteyiz.

Siber alanda karşılaşılan suç ve sorunlara karşı toplumun her düzeyinde birey ve kitlelerin bilinçlenmesi alınan ve alınabilecek tedbirlerin daha etkin sonuçlar doğuracağını ve doğurduğunu göreceğiz. Siber suçlara karşı topyekün tedbir ve eylem birliği içerisinde olması halinde etkin bir şekilde mücadele edilebilecektir. Bu bilinç de oluşa yazmaktadır (Connolly & Maurushat, 2013).

Ülkeler düzeyinde siber suçlar ile ilgili ortak tedbir ve tavır sergilenmesi gerekmektedir hal böyle iken tehdit, yapı ve tepkisel anlamda farklı görüş ve yaklaşımlar mevcuttur. Askeri önlem alınmasından yani savaş sebebi saymadan aynı şekilde ve aynı yöntemle karşılık verilmesine kadar farklı görüşler mevcuttur. Bu görüşler saldırıların nitelik ve kaynağı ile amacına göre değişebilmektedir.

Gelişmiş ve gelişmekte olan yani teknoloji ile irtibatı sıkı olan ülkeler siber tehditlere karşı siber güvenlik tedbirleri alınmaya çalışılmakla birlikte pek de başarılı olduğu söylenemez. Bunun nedeni olarak ortak tedbir kararı alınamaması, çıkar çatışmaları, yeterli yasal düzenlemenin yapılmamış olmasını söyleyebiliriz.

Bu doğrultuda elektronik ortamın "her anlamda sınırsız" bir ortam olması göz önüne alınırsa devletlerin kendi sınırları içerisinde gerekli ve yeterli düzenlemeler yapmasının yanında, değişik yasal ya da yönetsel düzenlemeleri içeren uluslararası ortak hareket edilebilecek anlaşma ya da platformlar oluşturulması gerekmektedir. Ancak bunun pek mümkün olmadığını ülkeler arasında da soğuk savaşın kalıntıları ve uluslararası çıkarlar bunun önündeki en büyük engeldir.

Türkiye'de de gelişmekte olan bir ülke olarak ancak ileri düzey teknolojik araçların kullanım oranı ile siber güvenlik alanında farkındalığın artması ve siber saldırıların kıskacında olması, bunun yanı sıra son dönemlerdeki stratejik konumunun ve siyasi tutumunun da beraberinde getirdiği siber güvenlik sorunsalına eylem planları, güvenlik programları, yasal

düzenlemeler, çalıştaylar, tatbikatlar yapılmakta olup; Emniyet Genel Müdürlüğü gibi güvenlik birimlerinin yanında Kamu Düzeni ve Güvenliği Müsteşarlığı, TÜBİTAK gibi kurumlar önlem ve çalışmalar yapmaktadır. Bunun yanı sıra ki en önemlisi toplumda yeterli düzeyde bilincin oluşturulması gerekmektedir. Tabi bu bilincin oluşması ve yerleşmesi için teknolojinin elde edilmesi ile elde bulunan teknolojinin sakınca ve zararlarının da farkındalığının oluşturulması gerekir.

Türkiye'de henüz yeni yürürlüğe giren 24.03.2016 tarih ve "6698 sayılı Kişisel Verilen Korunması Kanunu'nun" 1. Maddesinde kanunun amacı kişisel verilen işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ve uyacakları usul ve esasları düzenlemektir. Her ne kadar gerek Türk Ceza Kanunu' nun ilgili maddeleri gerekse başlı başına bir kanun olarak çıkan "Kişisel Verilerin Korunması Kanunu" olsa da kanunun onaylanmasından henüz 1 hafta sonra "Turkish citizenship database" (Türk vatandaşlık veritabanı) başlıkla yayınlanan ve yaklaşık 50 (49.611.709) vatandaşın kişisel verilerinin internet ortamında yasa dışı bir şekilde yayınlanması aslında geldiğimiz noktayı yüzümüze tokat gibi çarpmaktadır (Cumhuriyetarsivi.com, 2016). Çünkü verilerin yayınlanmasından sora yapılabilen tek şey ilgili siteye erişimi engellemek oldu. Avrupa Parlamentosu internete yüklenen veri tabanını "Bugüne kadarki en büyük kamuya ait bilgi sızıntısı" olarak niteledi. Bilgilerin yayınlandığı bilgisayarlar kimine göre Romanya kimine göre Kanada kimine göre de ABD merkezli… ama hangisi, belki hiçbirisi; cevabı muamma…cevaplar sadece ihtimaller ve olağan şüpheliler kıvamında…

Kaynağının ne olduğu bulunamasa da bu bilgilerle; ki kimlikte bulunan tüm bilgiler olması nedeniyle sahte kimlik çıkarılabilecektir. Dolayısıyla kredi çekilebilir, araç kiralanabilir, kefil olunabilir, telefon için sim kart alınabilir… Son dönemlerle birlikte bırakın kişisel verileri, güvenliğimizin, hak ve özgürlükler anlamında edinimlerimizin bile bu denli tartışıldığı bir ortamda kişisel verilerimizin güvenliğinin de elbet ifşa edilmesi pek şaşırtıcı olmasa gerek. Sadece bu konu için çözüm olarak belki de ilk adım olarak tüm vatandaşların kimlik numaraları yeni bir algoritma ile değiştirilip şifrelenip ardından her vatandaşa yeni bir kimlik sunulması gerekirken hiçbir tedbir dahi alınmaması bilgi çağında çağın gerisinde bile olduğunun farkında olmayan gelişmekte olan bir ülkenin yaşaması muhtemel bir sonuçtur.

Sonuç

Savunma amacıyla ortaya çıkan internet, bugün artık savunulamaz duruma düşmüş ve en büyük tehditlerden biri haline gelmiştir. İnternetin insanlığın bir parçası düzeyine ulaşması tarihte birçok yeniliğin insan hayatına yerleşmesine göre daha kolay ve hızlı olmuştur. Bilgi çağını da diğerlerinden ayıran temel farklılık da bundan kaynaklanmaktadır. Çünkü bilgiye ulaşmak da kolay, "bilginizi- bilgilerinizi" de kaybetmeniz de çok kolay bir hale gelmiştir. Bunun sonucu olarak, amacı daha hızlı paylaşım ile tam olarak doğru bilgiyi elde etmek olmasa da bilgiye sahip olmak amacıyla ortaya çıkan gelişen ve büyüyen siber ortamda bilgiyi paylaşmak ve bilgiye erişim güvenlik nedeniyle günden güne zor ve karmaşık noktalara gelmiştir. İnternette güvenlik nedenleriyle özgürlükler dengesi iyi korunmalı ve elektronik ortam kriz ortamına dönüştürülmemelidir.

Elektronik ortamın son dönemlerde hızla artması sonucu Dünya'nın nüfus sayısının yarısına yaklaşan internet kullanıcı sayısı son 20 yılın ekonomik düzenleyicisi konumunda olan küreselleşmenin geldiği ve bizi getirdiği noktanın fotoğrafıdır. Elektrik kesildiğinde hayatın seyri aynen devam ettirmeye çalışan insan, telefonunun şarjı bittiğinde kendini yalnız, kötü ve çaresiz hissedip panik yapması da durumun derinliğini de göstermektedir. Karşımızda gerçek dünyanın yanında bir de neredeyse gerçeği de içine alan bir siber dünya bulunmaktadır.

Elektronik ticaretin artması, nüfusun artması, internet kullanıcı sayısının ve kullanım çeşitlerinin artması aynı zamanda ödeme şekilleri gelişmesi gibi nedenlerle de desteklenmektedir. Gelişmekte olan bir ülke olarak ülkemizde bile kredi kartı ve banka kartı sayısı nüfusunu toplamının neredeyse iki katıdır. Elektronik ticaret hacmi 2015'te milyar TL ile ölçülürken bu rakam Dünya için trilyon dolar seviyesindedir. Elektronik ortam sanal olsa da gerçek işlemler ve gerçek bilgiler üzerinden yapılmaktadır. Dolayısıyla bazı tehdit ve çekinceleri de yanında getirmektedir. Elektronik ticarete taraf olan kişiler arasında güven tesis etmek bunun bertaraf edici ilk adımıdır. Çünkü 1990'lı yılların ortalarında hayatımıza giren elektronik ticaret sağladığı faydalarla getirdiği kolaylıklarla yaygınlaşmış günümüzdeki konumuna gelmiştir. Yanı sıra getirdiği olumsuzluklar önlenmesi zor tehditler oluşturmuştur. Karşımıza aşılmazı zor bir sorun olarak elektronik ortamda güvenlik sorununu da beraberinde sunmuştur. Her ortamda olabileceği gibi suç unsuru ve kötü niyetli 3. Kişiler elektronik ortamda da bulunmaktadır. Mali olarak hacmin ve çeşitliliğin fazlalığı ve bilgiye ulaşmanın kolaylığı ve en önemlisi Bilinçsiz tüketici ya da internet kullanıcısının varlığı da iştahlarını arttırmaktadır. Elektronik ortamda düşman askerler diyebileceğimiz çeşitlenmiş ve ayrı ayrı sürüme sahip virüs, Truva atı, kurtçuk, solucan zombi, spamlar, koyloggers ve casus

yazılımlar gibi tehditler mevcuttur. Bunu bilgilerinize ulaşmada, maddi menfaat edinmede ya da anti-virüs gibi ürünlere pazar oluşturma amacıyla olabilmektedir.

Elektronik ortamın gelişme hızına karşılık kişi, kurum ve yasal tedbirler açısından devletler aynı oranda güvenlik sağlayamaması siber saldırılara ancak cılız tedbirler alınabilmiştir. Bunun sonucu olarak siber dünyanın gerçek dünyaya galip gelmiş olabileceğini varsayabiliriz. Alınan en temel tedbir erişimi engelleme ya da yasaklama şeklinde olabilmekte ve da özgürlükler anlamında bazı sorunlara neden olabilmektedir. Alınan tedbirlerin güvenlik ile özgürlükler anlamında hassas bir denge kurmasını sağlayabilmesi esas olmalıdır. Gelişmiş ülkeler genel olarak tehdidi önleyici ve savunmayı güçlendirici "siber savunma kuvvetleri" oluşturmuşlardır. Ancak güvenlik anlamında uluslararası önlemlerin yeterince alınmaması daha doğrusu ulusal menfaatler nedeniyle bu önlemlerin alınamıyor olması tehdidi devletler düzeyine de taşımıştır. Öyle ki, ülkeler de birbirleri için siber saldırı tehdidi oluşturmaktadır.

Özellikle az gelişmiş ve gelişmekte olan ülkeler siber saldırılar için önemli bir hedef olarak görülebilmektedir. Bunun nedenleri arasında gelişmekte olan ülkelerin yapısal özellikleri sayılabilir. Tüketim eğiliminin fazlalığı ve bilinçsiz kullanım oranının yüksekliği en önemli açıklardır. Elektronik ticaretin gelişimine paralel bir hızda alınamayan teknik ve yasal önlemler nedeniyle suç ve suç unsurlarının artmasına neden olmuş ve önlenememektedir.

Türkiye Cumhuriyeti vatandaşının kişisel verilerinin internete sızdırıldığı öne sürüldü ve bu dikkate değer bir örnektir. Bu verilerin yayınlanmasının nedenleri tartışılamamış ve sonuçları basite indirgenmiştir. Alınacak teknik ve yasal tedbirleri yanı sıra önleyici ve de kötü sonuçlarını bertaraf edici düzenlemeler yapılmalıdır. Bundan sonraki çalışmalarda konu ile ilgili gelişmeler, alınması gereken tedbirler ve siber işlemlerin yıkıcı sonuçları üzerine daha detaylı çalışmalar yapılabilir.

Kaynakça

B.S. Sahay (2003). Understanding trust in supply chain relationships. *Industrial Management & Data Systems*. 103(8) (pp.553 – 563).

Connolly, C., Maurushat, A. (2013,July). An Overview of International Cyber-Security. http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_reportoverview_intnl_cybersecurity_awareness.pdf (Erişim tarihi: 20 Temmuz 2013).

Elektronik Ticaret Koordinasyon Kurulu Hukuk Çalışma Grubu Raporu . (1998, Mayıs). http:// www.etkk.gov.tr (Erişim tarihi: 15 Şubat 2016).

Fisher, D.J. (2003). *An Investigation into the Attitudes Towards and Participation in Online Instruction Among Higher Education Business Education Faculty at NABRE Institutions :A Ten Year Comparison.* Missisipi State University, *Doctoral Dissertations*, (Umi Microform number:3080194).

İlbaş Ç., Köksal M. (2011) *Türkiye Bilişim Suçları Raporu* 1990-2011. İzmir: Uluslararası Bilişim Hukuku Kurultayı 17/11/2011 - 19/11/2011.

Kenneth, G. A.g.m. (2010) : Ünver, M. ve Canbay, C, *Ulusal ve Uluslararası BoyutlarıylaSiberGüvenlik.*
*h*ttp://www.emo.org.tr/ekler/a9a502d6e646c25_ek.pdf?dergi=598 (Erişim Tarihi: 11 Nisan 2012)

McCole, P. (2002). *The Role of Trust for Electronic Commerce in Services*.International Journal of Contemporary Hospitality Management.14(2)(pp.s.82).

Marshall, M. ve Powers, B.R. (2015). *Global Köy*. İstanbul: Skala Yayınları.

Solomon, M., Bamossy, G., Askegaard, S. Ve Hogg, M. (2002).*Consumer Behaviour: A European Perspective*.England: Pearson Education.

http://www.cumhuriyetarsivi.com/katalog/192/sayfa/2016/4/5/14.xhtml (Erişim Tarihi: 01 Mayıs 2016)

TİM, Ekonomi Dış Ticaret Raporu.http://www.tim.org.tr/tr/ihracat-arastirma-raporlari-ekonomi-ve-dis-ticaret-raporu-1.html (Erişim Tarihi: 15 Şubat 2016).

Türk Ticaret Kanunu. http://www.mevzuat.gov.tr (Erişim tarihi: 22 Nisan 2016).

United States-China Economic and Security Review Commission, http://www.uscc.gov (Erişim Tarihi: 10 Aralık 2008).

Uysal ve Tunç (1996). *Basic ile Programlama*. İstanbul: Teleteknik Yay.

Wibowo, R., Japarianto, E. (2013). *Pengaruh Retail Mix Terhadap Mınat Beli Di Keraton Department Store Jurnal Manajemen Permasaran*,1(1)(pp 1-12)

Yeni Ekonomi (2001). *NTV MAG Dergisi*, s.87.

Yılmaz, S. ve Salcan O. (2008). *Siber Uzay'da Güvenlik ve Türkiye*. İstanbul: Milenyum Yayınları

http://www.wto.org (Erişim tarihi: 15 Şubat 2016).

http://www.dijitalajanslar.com/internet-ve-sosyal-medya-kullanici-istatistikleri-2015 (Erişim Tarihi: 22 Nisan 2016).

http://www.ito.org.tr/itoyayin/0016184.pdf (Erişim tarihi: 22 Nisan 2016).

http://www.eticaret.com/blog/dunyada-ve-turkiyede-e-ticaret-pazar-buyuklugu (Erişim tarihi: 22 Nisan 2016).

http://www.academia.edu/5191271/G7den_G20ye_Giden_Yol_ve_G20_ile_%C4%B0lgili_Temel_Unsurlar (Erişim tarihi: 21 Nisan 2016).

http://www.egm.gov.tr (Erişim tarih: 15 Mart 2016).

http://www.resmigazete.gov.tr (Erişim tarihi: 26 Nisan 2016).

http://www.cyber-warrior.org/Forum/turkiye-de-bilisim-ve-siber-suc-kavrami_509898,0.cwx (Erişim tarihi: 21 Nisan 2016).

http://www.tuik.gov.tr (Erişim tarihi:19 Nisan 2016a).

http://www.tuik.gov.tr (Erişim tarihi:12 Şubat 2016b).