Kamu Yönetimi ve Politikaları Dergisi
Journal of Public Administration and Policy
Araştırma

BİLGİ TOPLUMU, SİBER GÜVENLİK VE TÜRKİYE UYGULAMALARI

INFORMATION SOCIETY, CYBER SECURITY AND TURKEY

Ceray Aldemir[1]

Merve Kaya[2]

Öz

Küreselleşmenin beraberinde getirdiği kavramlardan biri olan bilgi toplumu, içinde bulunduğumuz teknoloji temelli bu dönemde hayatımızın bir parçası haline gelmiştir. Bilgi temelli oluşan bu toplum düzeninde bilginin üretilmesi, işlenmesi, kullanılması gibi hususların önemi anlaşılmış ve bu alanlar ile ilgili çeşitli hedefler oluşturularak politikalar geliştirilmiştir. Bu doğrultuda karşımıza çıkan diğer bir kavram, bilginin korunması ve kötüye kullanımına yönelik geliştirilen güvenlik stratejilerini ifade eden siber güvenlik kavramıdır. Siber güvenlik kavramı hem birey hem de kurum bazında, ilgili tedbirlerin alınması ve muhtemel kayıpların önüne geçilmesi yönünde dikkatle incelenmesi gereken bir konudur.

Bu çalışmada nitel veri analiz yöntemlerinden biri olan literatür analizi aracılığı ile bilgi toplumu kavramı bağlı olduğu kavramlar ile birlikte incelenmiştir. Buna ek olarak Türkiye'de bilgi toplumu düzeyine erişme ve siber güvenliği sağlamak için atılan adımlardan bahsedilmiştir. Araştırma sonucunda, bu iki kavramın gerekliliklerini yerine getirilebilmek, bilgi toplumu çağında var olabilmek için; Türkiye'de alınan önlemlerin geliştirilmesi, alana verilen önemin arttırılması ve yasal düzeneklerin iyileştirilmesi gerekliliği kanısına varılmıştır.

Anahtar Kelimeler: Bilgi Toplumu, Bilgi Güvenliği, Siber Güvenlik, Türkiye'de Bilgi Toplumu, Türkiye'de Siber Güvenlik.

Abstract

Information society, which is one of the concepts brought by globalization, has become a part of our life in this technology-driven period. In this knowledge-based society, the importance of issues such as the production, processing, and use of information has been understood and policies have been developed by creating various targets related to these areas. Another concept that we encounter in this direction is the cyber security, which expresses the security strategies developed for the protection and abuse of information. The concept of cyber security is an issue that needs to be carefully examined to take relevant measures and prevent possible losses, both on an individual and corporate basis.

In this study, the concept of information society has been examined together with the concepts it is connected through the literature analysis, which is one of the qualitative data analysis methods. In addition, the level of access to the information society in Turkey and the steps taken to ensure cyber security have been discussed. As a result of this research, in order both to fulfill the requirements of these two concepts, and to exist in the age of information society; Turkey needs to increase and improve the legal regulations.

Keywords: Information Society, Information Security, Cyber Security, Information Society in Turkey, Cyber Security in Turkey.

[1]Dr. Öğretim Üyesi, Muğla Sıtkı Koçman Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Kamu Yönetimi Bölümü, cerayaldemir@mu.edu.tr, ORCID: 0000-0002-7996-4886

[2]Yüksek Lisans Öğrencisi, Muğla Sıtkı Koçman Üniversitesi, Sosyal Bilimler Enstitüsü, merve.kaya9511@gmail.com, ORCID 0000-0002-0667-9582

Makale Geliş Tarihi: *24 Nisan 2020* ***Makale Kabul Tarihi:*** *14 Haziran 2020*

I. GİRİŞ

Teknoloji, bir süreç tarihi olan insanlık tarihinin başlangıcından beri tarihte kendine yer edinmiştir. Bu durumun bir göstergesi de bugün içinde bulunduğumuz dönemin temel dayanaklarının tekerleğin icat edilmesi, ateşin keşfedilmesi gibi olgulara dayanmasıdır. Tarihte oluşum gösteren ilk toplumlardan bugün içinde yaşadığımız bilgi ve teknoloji temelli toplum düzenine geçiş, toplumsal yapının dinamik bir temele sahip olduğunu kanıtlar (Çalık ve Çınar, 2009: 77-78).

Değişen ve gelişen toplum olgusu, teknolojiyi de beraberinde dönüşüme uğratarak bugün karşımıza sıklıkta çıkmakta olan bilgi toplumu ve siber güvenlik kavramlarını hayatımıza dahil etmiş, günümüzün ve geleceğin en önemli konuları arasında yer almasına neden olmuştur (Yılmaz vd., 2015: 133). Yeni toplum düzeni içerisinde ekonomik temelde var olabilmek için bireylerin ve toplumların değişime ayak uydurabilme potansiyelini taşıması, kendini revize edebilmesi gerekir (Bedir, 2002: 62). Kendi kendine yeten toplum algısı, küreselleşmenin getirdiği bilgi toplumu çerçevesinde artık geçerliliğini koruyamayacak, yeniliklere açık ve kendini geliştirebilen toplumlar süreci başarılı ile tamamlayabileceklerdir (Balay, 2004: 77). Bilgi toplumu seviyesini yakalamak, değişime ayak uydurabilmek, bilgi temelli toplum oluşturabilmek bu kadar önemliyken, bilgiye erişmek ve üretip kullanmak kadar bilgi güvenliğinin sağlanması da en temel hedeflerden biri halini almıştır (Özdemirci ve Torunlar, 2018: 79).

Bu çalışmanın amacı, geçmişten günümüze evrilerek gelen bilgi toplumu olgusunu açıklamak ve çağımızın en önemli problemlerinden biri olan siber güvenlik kavramı ile arasındaki bağı Türkiye özelinde incelemektir. Bu bağlamda çalışma üç kısımdan oluşmaktadır. İlk kısımda çalışmanın temelini oluşturan kavramlar tanımlanmıştır. İkinci kısımda Türkiye'nin bilgi toplumu içerisindeki konumu hakkında bilgi verilmiştir. Üçüncü kısımda ise Türkiye'de siber güvenlik politikaları, uygulamaları ve alınan önlemlere değinilmiş, verilen tüm bilgiler ışığında bir değerlendirme yapılarak alan nezdinde öneriler ortaya konulmuştur.

1. Kavramsal Çerçeve

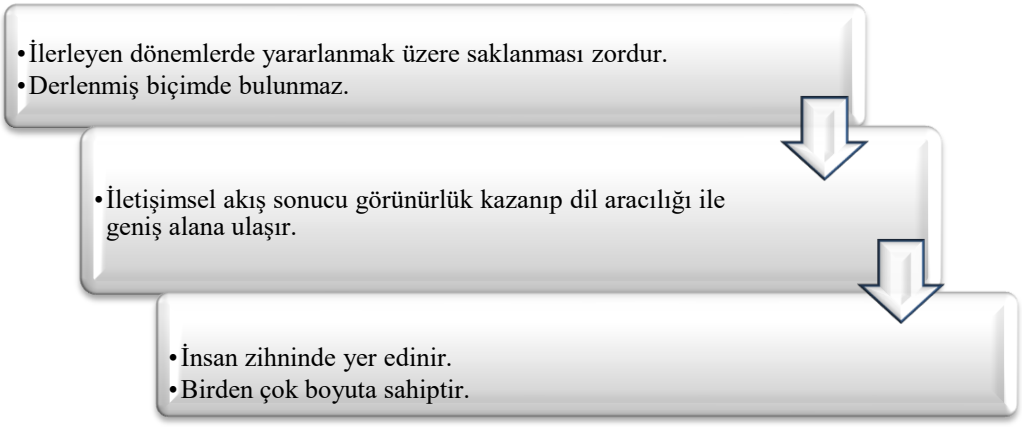
Çağımızın en önemli kavramlarından biri olan bilgi ve beraberinde getirdiği olguların hem bireyi hem de bireylerden oluşan toplumu dönüşüme uğratan ve geliştiren bir olgu olduğu bilinmektedir. Bu bölümde hem günlük hayat akışı içerisinde hem de istihdam, eğitim, hizmet, teknoloji gibi birçok alanda sıklıkla karşımıza çıkan bu kavramların ne anlama geldikleri ve tarihsel arka planlarına değinilmiştir. Ele alınan kavramlar ise bilgi, bilgi toplumu, bilgi güvenliği ve bağlantılı olduğu siber güvenlik kavramlarıdır.

1.1. Bilgi. Dahil olduğu alanlar ve kültürler farklılaştıkça anlamı da değişen bilgi kavramı için tek bir tanımlama bulunmamakta, ancak üzerinde görüş birliğine varılan "*mantıklı bir yargı ya da*

deneysel bir sonuç sunan, başkalarına sistemli şekilde bir iletişim aracıyla ulaştırılan, olgulara ya da düşüncelere ilişkin düzenli ifadeler dizisidir" şeklindeki ifade literatürdeki yerini almaktadır (Bell, 2013: 175). Uçak (2010: 707)'a göre ise bilgi kavramının tanımlanmasında üzerinde durulacak olgular bireyin zihinsel sistemi içerisinde bulunan yapı ve bu yapıya bağlı olarak iletim işlevinin gerçekleşmesi hususlarıdır. Farklı bir perspektiften bakıldığında ise mesajın iletilmesi için kullanılan hem iletişim kanalının hem alıcının bir fonksiyonu, bazen de kaynağın bir fonksiyonu olan ve veri (data) olarak ifade edilen bir kavram olarak karşımıza çıkar (Orkan, 1992: 93).

Veri, belli bir olguya ait ağırlık, hacim, uzunluk gibi nicel ya da sembol, resim, ses gibi nitel kayıtlar bütünü (Kitchin, 2014: 2-4) olarak nitelendirilebilen kavramdır. Veri kelimesi ile genel olarak anlatılmak istenen enformasyona dönüşecek basit olgu olduğu ve enformasyon ile beraber ele alındığı zaman sonucunda bilgiye ulaşılacağıdır. Enformasyon ise verilerin belli bir amaç doğrultusunda bir araya getirilmesi ile oluşur (Yılmaz, 2009: 98). Toparlanacak olursa enformasyon işlenmiş bir veri, bilgi ise zihinsel kurgularla, değerlendirme, karar verme, tahmin yürütme gibi süreçler sonunda kullanılabilir enformasyon olarak karşımıza çıkmaktadır (Durna ve Demirel, 2008: 132-134). Bu anlatılar ışığında diğer bir tanımlama ise *"sonuçlara, kavramlara, yorumlara, fikirleri gözlemlere ve yargılara bağlı kişiselleşmiş enformasyonlardır"* biçiminde literatürdeki yerini almaktadır (Alavi ve Leidner, 2001: 109).

Şekil 1: Bilgi Kavramının Özellikleri



Kaynak 1: Özsağır (2013: 76)'dan uyarlanmıştır.

1.2. Bilgi Toplumu.İnsanlık ve toplum olguları tarih boyunca belli dönemlerden geçerek varlığını günümüze kadar ulaştırmıştır. Bilgi toplumu kavramı ve özelliklerine geçmeden önce yaşanılan dönemleri ana hatlarıyla belirtmek sürecin algılanabilmesi açısından yararlı olacaktır.

Yaşanılan dönemlerden ilki, bireyin kendisine yetecek kadar bir hayat tarzını benimsediği, temel amacının fizyolojik ihtiyaçlarını karşılamak ve üretimin yok denecek seviyede az olduğu avcılık

toplayıcılık dönemidir (Kutlu ve Taban, 2007: 4-5). Beslenme ihtiyacı avlanma ile karşılanırken, barınma ihtiyacı için çözüm mağara ve ağaç kovuklarında bulunmuştur (Fındıkçı, 1997: 41). Alım-satım ilişkisinin temeli ise takasa dayanmakta (Mayor, 2013: 229). Toprağın işlenmeye başlanması ile birlikte hayat tarzında değişiklikler yaşanmış, köy denilen yerleşim yerleri oluşturulmuş ve tarım toplumu ortaya çıkmıştır (Yılmaz, 2006: 4). Teknoloji ile yavaş yavaş tanışılmaya başlanmış ve üretim toprağa dayalı biçimde artmaya başlamıştır (Erkan, 1998: 134). Bu durum da beraberinde ekonominin para ve üretilen tarımsal ürünlerin değiş tokuşuna dayanmasına yol açmıştır (Arklan ve Taşdemir, 2008: 69).

Sanayi devrimi ile geçilen yeni dönemde ekonomik, sosyal, siyasal ve kültürel hayatta değişiklikler meydana gelmiş, yeni hayat tarzı ve üretim ilişkileri gelişmiştir (Erkan, 1994: 3). Üretimin fabrika düzeyine erişerek büyük oranda gelişme göstermesi, beraberinde pazar arayışını, sömürgecilik olgusunu ve sosyal sınıf oluşumunu getirmiştir (Çalık ve Çınar, 2009: 82). Bu dönemde emek yoğun üretim şekli, yerini makine gücüne devretmiştir (Özdemir, 2014: 6). Gelişen teknoloji, yeni hayat tarzı ve makineleşme gibi olgular, sanayi toplumunu revizyona uğratarak farklı bir döneme geçilmesi ihtiyacını doğurmuş, bu yeni toplum düzeni ise bilgi toplumu kavramı çerçevesinde hayat bulmuştur (Erkan, 2004: 205). Tarım toplumundan sanayi toplumuna geçiş, sanayi toplumundan bilgi toplumuna geçiş kadar hızlı gerçekleşen bir olgu değildir. Bunun sebebi ise gelişen teknoloji ile beraber bilinçlilik düzeyi artan bireylerin bu sürece daha kolay adapte olabilir hale gelmesinde yatmaktadır (Çalık ve Çınar, 2009: 82-83).

Yeni toplum düzeni olan bilgi toplumu, gelişen teknoloji ile beraber bilgi odaklı sermaye ve buna bağlı olarak bilgi sektörünü oluşturan, alanda uzmanlaşmış insan unsurunu önemli hale getiren, üretim sürecinde bilgiyi ön plana çıkaran, eğitim sürecinin dönemsel değil ömür boyu olduğu bir süreci ifade etmektedir (Aktan ve Vural, 2016: 3). Para ve sanayi temelli ekonomik düzen yerini bilgi ve dijitalleşmeye dayalı düzene devrederken, temeli makineye dayanan altyapı ise kaynağını araştırma ve geliştirmeye dayandırmış, bu durumun bir sonucu da büyük fabrikaların yerini ofis ortamlarının alması olmuştur (Alpaslan ve Kutanis, 2007: 59).Bu toplum yapısı, *"Fritz Machlup tarafından "bilgi ekonomisi", Rolf Dahrendroff tarafından "post-kapitalizm", Masuda tarafından "Information Society" ve Daniel Bell "post-indüstriyel" dönem*" olarak adlandırılmıştır (Erkan, 1994: 71-72).

İçerisinde barındırmış olduğu bu özellikler sayesinde istihdam da artık sanayi toplumunda yapılanan meslekler aracılığı ile gerçekleşemeyecek hale gelmiştir (Kocacık, 2003: 5). Yeni meslek yapılarının gerektirdiği bu toplumda bilginin üretiminden dağıtımına kadar görev alan işçiler Drucker tarafından "bilgi işçisi" olarak nitelendirilmiş ve öğrenme ve araştırmaya meraklı, var olan soruna karşı çözüm üretme potansiyeline sahip olan, yeniliğe açık üretken bireyler bu kavram perspektifinde ele alınmıştır (Drucker, 1994: 186).

Şekil 2: Sanayi ve Bilgi Toplumu Arasındaki Farklar

Konu	Sanayi Toplumu	Bilgi Toplumu
Sermaye	Maddi sermaye	Bilgi ve insan sermayesi
Dönem Başlangıcı	Buhar Makinası	Bilgisayar
Güç Kaynağı	Kol gücü	Beyin gücü
İnsan Kaynağı	Fiziksel insan sermayesi	Nitelikli insan sermayesi
Ürün	Sanayi mal ve hizmetleri	Bilgi ve teknoloji üretimi
Üretim Alanı	Fabrikalar	Bilgi ağları ve veri bankaları
Dönemsel Etkiler	İşsizlik	İşgücü tasarrufu
Eğitim ve Bilgi Kaynağı	Genel ve temel nitelikteki eğitim	Bireysel ve sürekli eğitim
Sektörler	Tarım, sanayi ve hizmetler sektörleri	Bilgi sektörü
Üretim Faktörleri	Emek, tabiat, sermaye, girişimci	Sanayi faktörlerine ek olarak bilgi faktörü
Yönetişim	Temsili demokrasi	Katılımcı demokrasi

Kaynak 2: Aktan ve Vural (2016: 4-5)' dan uyarlanmıştır.

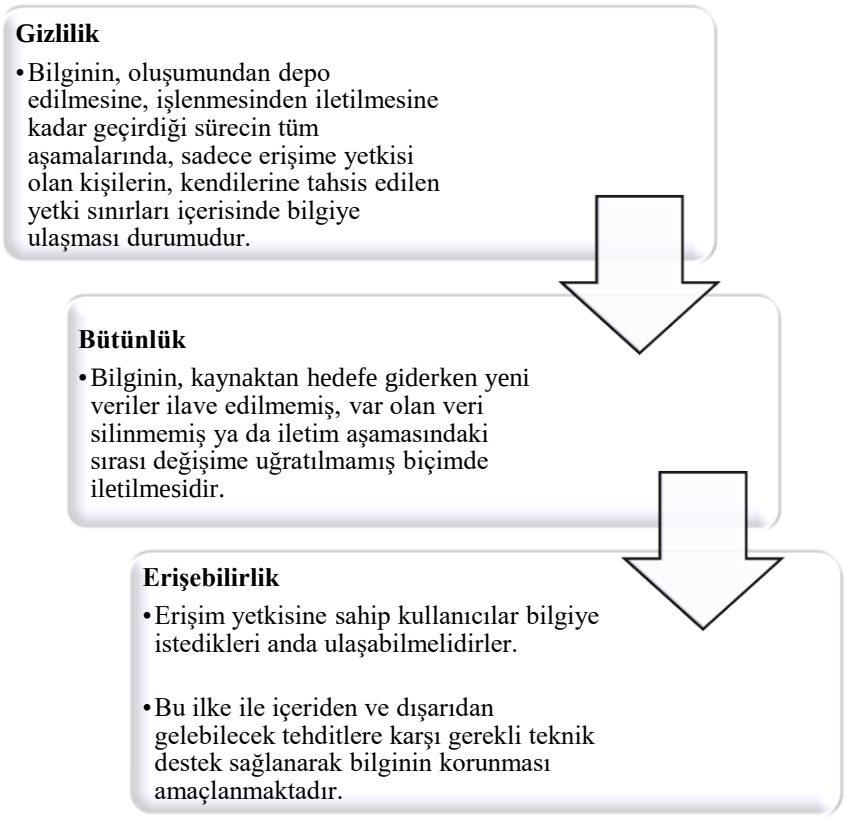
Bilgi toplumu düzeni, yaşamı oldukça kolaylaştırıp profesyonelce gelişen bir hayat tarzı sunmasına karşın, devletin bilgi tekeline sahip olması, devlet gücünün merkezileştirilmesi, toplumda bilgi eliti denen, bilgiye ulaşım kolaylığını elinde bulunduran, gerekli ekipman ve teknik donanım maliyetine katlanabilen bir kesimin oluşması, bilginin kolay elde edilebilmesinden kaynaklı kişisel hakların risk altında bulunması, erişim kolaylığından kaynaklı bilginin kötü amaçla kullanılabilmesi, bilgisayar karşısında uzun süre kalmaktan kaynaklı göz bozukluklarının oluşabilmesi, gelişmiş ve gelişmemiş ülkeler arasında eşitsizlik yaratması gibi sorunlara yol açabilmektedir (Şanlısoy, 1999: 171-179).

1.3. Bilgi Güvenliği. 1990'lı yıllara tekabül eden ve dünyanın her yerinde yaşanan teknolojik gelişmeler, bilgi ve bilgi tabanlı sistemlerin yaygınlaşması, yoğun internet kullanımı gibi olgular bilginin korunması hususundaki hassasiyet gün geçtikçe açığa çıkarmaktadır (Clarke ve Knake, 2010: 74-85; Aktaran: Aslay, 2017: 24). Hayatımızın her alanına nüfuz eden interaktif akış, beraberinde bankacılık hizmetleri, kamu hizmetleri gibi sistemlerin dijital ortamda kullanımını ve bu sistemlerin de saldırıya açık bir hedef halini almasını getirmiştir (Doherty vd., 2009: 449-450). Özel ya da kamusal olmak üzere her alanda işlenen, dönüştürülen ve kullanılabilen, en önemli üretim faktörlerinden biri olan bilgi, gerekli tedbirler alınarak iletilmesi gereken noktaya kadar, siber güvenlik tehditlerinden arındırılarak güvenle taşınmalıdır (Vural ve Sağıroğlu, 2008: 3).

Bilgilere, yetki kapsamı dışında ulaşılıp kullanılması, ortaya çıkarılması, silinmesi, değiştirilmesi veya zarar verilmesi kısaca kişisel veya kurumsal mahremiyeti, bütünlüğü ve ulaşılabilirliği ihlal eden olguların öne geçilmesine bilgi güvenliği denilmektedir (Baykara vd., 2013: 231-232). Bilgi güvenliği, sadece edinilen bilginin kötüye kullanılmamasını değil, edinildiği kaynağın yasal olması, iletim aşamasındaki kanalların güvenli olması ve gerektiği zaman güvenli bir şekilde yok edilmesi unsurlarını da kapsayan bir sürecin ifadesidir (Eminağaoğlu ve Gökşen, 2009: 7-9).

Bilgi güvenliği kavramı, içerisinde gizlilik, bütünlük, erişilebilirlik gibi üç ana unsuru (Saltzer ve Schroeder, 1975: 1280) ve buna ek olarak kayıt tutma, kimlik tespiti, güvenirlik, inkâr edememe gibi yan unsurları barındıran bir kavramdır (Tekerek, 2008: 133). Bu çalışmada kavramın temel üç ana unsuru olan gizlilik, bütünlük ve erişilebilirlik kavramları ele alınmıştır.

Şekil 3: Bilgi Güvenliği Kavramının Unsurları



Kaynak 3: Yılmaz, (2013: 15); Peltier, (2005: 39); Tekerek, (2008: 133) 'den uyarlanmıştır.

Bilgi güvenliğinin sağlanması için tüm unsurlar titizlikle kontrol edilip gerekli tüm teknik destek sağlansa dahi, insan unsurunun bu sürecin hem en önemli hem de en zayıf halkası olduğu göz ardı edilmemelidir(Yılmaz, 2013: 18). Bilgi güvenliği ile ilgili gerekli tüm eğitimler hem özel kuruluşlar hem de kamu kurumları tarafından çalışanlara verilmeli, tedbirler üst seviyeye çıkarılarak yaşanabilecek maddi ve manevi kayıplar önlenmeye çalışılmalı, kurum içerisinde istihdam edilen

personelin hatalı davranışları ve ihlalleri yüzünden bilgi güvenliğinin sekteye uğraması engellenmelidir (Vural ve Sağıroğlu, 2008: 5).

1.4. Siber Güvenlik. Gelişen teknoloji, getirdiği yenilikler, bilgisayar kullanımının giderek artması, internetin hayatımızın bir parçası haline gelmesi, yönetim ve hizmet anlayışının dijital ortamda kendini revize etmesi, gündelik hayat akışının elektronik ortama taşınması gibi olgular her türlü dijital ortamı içinde bulunduran, sanal bir ortam olan, kara, deniz, hava ve uzaydan farklı bir olgu olma özelliği taşıyan siber uzay (siber ortam, siber alan) da hayat bulmuş olgulardır (Akyazı, 2013: 216). İlk olarak 1982 yılında William Gibson tarafından "*Burning Chrome*" adlı eserde görünürlük kazanan siber uzay kavramı (Libicki, 2009: 12-13), sadece internet temelli ağları değil, iletişim temelli cep telefonları, telsiz sistemleri, uçaklar ve insansız hava araçları gibi bilgi sistem teknolojilerini kullanan kapalı ağlar dahil tüm ağları kapsamaktadır (Çifçi, 2013: 5).

Dijital imkanların birey, kurum, devlet gibi aktörler tarafından tüm alanlarda kullanılmasıyla birlikte, bilginin olduğu her ortamın bir hedef haline geldiği siber uzayda, bilgi güvenliğinin sağlanması kapsamında alınacak tedbir ve önlemler siber güvenlik kavramını ortaya çıkarmıştır (Choucri, 2012: 5; Aktaran: Tarhan, 2017: 5). Siber güvenlik olgusu bütünlük, gizlilik ve erişilebilirlik unsurlarının bir arada bulunduğu bilgi güvenliğini sağlamak adına atılan olgular bütünü olarak kavramsallaştırılır (Hekim ve Başıbüyük, 2013: 137).

Türkiye'nin "*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"* içerisinde siber güvenlik kavramı için yapılan tanımlama, bilişim sistemlerinin birleşerek oluşturduğu ve siber ortam olarak kavramsallaşan ortamı, saldırıları tespit etmek suretiyle kayıplardan korumaya, saldırının tespiti halinde gerekli teknik desteği devreye sokmaya ve saldırı öncesi konuma geri döndürmeye odaklı stratejiler bütününe verilen addır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013-2014: 9).

Siber saldırı ise *"2016-2019 Ulusal Siber Güvenlik Stratejisi*' ne göre, siber uzay denilen boyutun içerisindeki tüm sistemlere, bilgi güvenliği unsurlarının kişi ya da sistem nezdinde bilinçli olarak ihlal edilmesi sonucu yapılan kötü amaçlı müdahaleleri kapsamaktadır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019: 8).

Bu kötü amaçlı müdahaleler, sisteme yetkisi dışındaki kişilerin erişimi, bilgilerin çalınması, ifşa edilmesi, değiştirilmesi veya yok edilmesi, cihazlara kullanıcının yetkisi dışında virüs bulaştırılması, hesaplara ilişkin şifrelerin çalınması, bireylere "spam" denilen istenmeyen e-postaların yollanması, saldırganın bireyi kendi isteği doğrultusunda hareket etmesine neden olan sosyal mühendislik saldırısı başta olmak üzere çok çeşitli müdahaleleri kapsamaktadır (Rittinghouse vd., 2003: 334). Bu saldırıların önüne geçilmesi ve güvenli bir dijital ortam sağlanması hedefleri ışığında hükümetler, şeffaflık unsuru çerçevesinde gerekli ağlara erişimin sağlanması, bireylerin çevrimiçi

ortamlardaki haklarına saygı gösterilmesinin gerçekleştirilmesi ve internet ortamında güven unsurunun görünürlük kazanması gibi olguları hedeflemektedirler (Önen ve Kurnaz, 2017: 733). 2017 yılında ABD'nin bütçe içerisinden 13,152 milyar dolar gibi büyük bir miktarı siber güvenlik alanına tahsis etmesi, politika hedefleri ve alanın önemi kapsamında verilebilecek örnekler bir tanesidir (Aldemir ve Şen, 2019: 1570).

Siber güvenlik olgusunun önemini kavrayabilmek adına küresel düzeydeki saldırılar ve yol açtığı maddi/manevi kayıplar kapsamında verilebilecek ilk örnek Estonya' da gerçekleşen siber saldırıdır. 2007 yılının Nisan ayı sonlarına doğru Estonya, bankalar, medya şirketleri, devlet kurumları gibi ülkenin temel taşı niteliğinde olan birçok kurum ve kuruluşu hedef alan çok büyük bir siber saldırıya maruz kalmıştır (Traynor, 2007; Aktaran: Bıçakçı, 2012: 215). Hem kamuya ait hem de özel yapılanmaya sahip internet sitelerinin çökmesiyle ülkenin sahip olduğu iletişim ve e-devlet altyapısı kullanılamaz hale gelmiş, bunun yanı sıra ticaret alanında gerçekleşen etkinlikler kesintiye uğramıştır (Kara, 2013: 47-48). Verilebilecek diğer bir örnek ise 2010 yılındaki "*Stuxnet"* saldırısıdır. Bu saldırının 2010 yılının Haziran ayında İran'ın sahip olduğu nükleer tesislere kadar ulaştığı ve nükleer bazlı faaliyetleri yavaşlatıp neredeyse durdurduğu bilinmektedir (Langner, 2011: 49-50)

Sony firmasına ise 2014 yılında kendi yapım firmasınca yayınlanması tasarlanan Kuzey Kore lideri Kim Jong-un' u hedef alan ve suikast konusu ile gündem yaratan "*The Interview*" (Röportaj) filmine dayalı bir saldırıya maruz kalmıştır. Bu saldırı maddi temelde görülen hasarın yanında, bireylerin düşünce ve buna dayalı olarak eyleme döktükleri ifade olgusunu sınırlaması gerekçesiyle büyük ses getirmiştir (Keleş ve Sal, 2013: 33-34). Anonymous grubu tarafından gerçekleştirilen ve *"OpIsrael"* adı ile anılan siber saldırı ise, Gazze olayı temelinde binlerce İsrail hükümet yetkilisinin kişisel hesapları, İsrail Savunma Kuvvetleri ve İsrail'e ait kamu kurumlarının siteleri etkisiz hale getirilmiştir (AA, 2012).

Oluşabilecek muhtemel kayıpların önüne geçilmesi adına siber saldırıların hedefi halinde bulunan bireyler ve kurum personellerinin, alacağı eğitimler sayesinde konunun önemi hakkında gerekli bilince sahip olmaları sağlanmalıdır (Yılmaz vd., 2015: 143). Siber saldırının önüne geçmek için verilen savaşta hem kamu hem de özel sektör uyum içinde çalışmalı, yazılımlar milli nitelik kazandırılarak daha güvenli hale getirilmeli, hız kavramı göz önünde bulundurularak değişime uyum sağlanmalı ve yasal nitelikteki oluşumların güncelliği korunmalı, hizmet akışının kesintiye uğrayabilmesi ihtimaline karşı devreye sokulacak bir risk planı oluşturulmalıdır (Öğün ve Kaya, 2013: 171-173).

II. Türkiye'nin Bilgi Toplumu İçerisindeki Konumu

Küresel düzen içerisindeki her ülkede 20. Yüzyılın ikinci yarısından itibaren bilgi toplumu seviyesine ulaşma adına adımlar atılmaya başlamıştır (Ezer, 2018: 21). Türkiye de bu amaç doğrultusunda politikalar geliştirmiş ve bilgi toplumu olma yolunda yadsınamayacak kadar büyük adımlar atmıştır (Çukurçayır ve Çelebi, 2012: 67).

Bu adımlar ise, T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Bilgi ve İletişim Teknolojileri Dairesi, (2020) tarafından şu şekilde ifade edilmiştir:

- Ülkemiz ve Dünya Bankası beraberliğinde oluşturulan "*Bilişim ve Ekonomik Modernizasyon Raporu"* (1993)
- Ulaştırma Bakanlığı ve TÜBİTAK iş birliğinde gerçekleştirilen "*Türkiye Ulusal Enformasyon Altyapısı Ana planı (TUENA)"* (1999)
- Dış Ticaret Müsteşarlığının başkanlığını üstlendiği "*Elektronik Ticaret Koordinasyon Kurulu"* (1998-2002),
- Başbakanlık Müsteşarının başkanlığını üstlendiği *"Kamu-Net Üst Kurulu ve Kamu-Net Teknik Kurulu"* (1998-2002),
- *"e-Türkiye Girişimi"* (2001)
- *"e-Dönüşüm Türkiye Projesi"* (2002-…) ve bu projenin hayata geçmesini sağlamak adına "*Bilgi Toplumu Dairesi*"" nin kurulması (2003) ve sonucunda oluşturulan "*2003-2004 Kısa Dönem Eylem Planı"*
- "*2003-2004 Kısa Dönem Eylem Planı"* tamamlandıktan sonra ise "*2005 Eylem Planı"* ve ardından *"2006-2010 Bilgi Toplumu Stratejisi ve Eylem Planı"*
- *"2014-2018 Bilgi Toplumu Stratejisi ve Eylem Planı"*

Tüm bu gelişmelerin, planların ve oluşumların yanı sıra kamuya ait hizmetlerin bürokratik engelleri ve zaman alan prosedürleri aşarak hızlı ve güvenli bir şekilde dijital ortama taşınması işlevini yerine getiren "e-devlet kapısı" uygulaması, bilgi toplumu olma adına gerçekleştirilen faaliyetlere verilebilecek en güzel örnektir (İşbilen, 2016: 77; Ulusoy ve Karakurt, 2002: 135). "*Kamu Bilgi ve İletişim Teknolojileri Yatırımları*" raporu incelendiği zaman, 2019 yılına ait yatırımların 2 milyar 693 milyon TL olduğu ve bu yatırımların büyük bir oranının, e-devlet hususunda önemli adımlar atan Adalet Bakanlığı, İçişleri Bakanlığı gibi kurumlara tahsis edileceği öngörülmektedir (Kamu Bilgi ve

İletişim Teknolojileri Yatırımları, 2019: 1-2). Birleşmiş Milletler tarafından hazırlanan *"e-devlet Kalkınma Endeksi"* 2018 verilerine göre ise Türkiye, bilgi ve iletişim teknolojileri temelinde yaşanılan ilerlemeler ve ülkedeki bireylerin bu ilerlemeye sağladığı adaptasyon bazında 193 ülke içinde 53. sırada yerini almaktadır (TÜİK, 2020b)

Ancak karşımıza çıkan durum, gelişen teknoloji ve yaşanılan hızlı dönüşüm süreciyle beraber gelinen seviye olan bilgi toplumu düzeyine ulaşabilmek için yeni politikalar hayata geçirmesi gerektiği ile ilgilidir (Bozkurt, 2000: 214). Uluslararası Telekomünikasyon Birliği tarafından hazırlanan, *"Bilgi ve İletişim Teknolojileri Gelişmişlik Endeksi"* değerlerine göre 2017 verileri incelendiği zaman, Türkiye'nin 176 ülke içinde 67. sırada olduğu görülmektedir (TÜİK, 2020c). Bilgi toplumu düzeyine erişebilmenin teknolojiye yapılan yatırımlara, üretimlere ve bu alanda lider haline gelen rakiplerle rekabet edebilir hale gelmeye bağlı olduğu durumda, Türkiye'de alan ile ilgili yeterli üretim yapılamamaktadır (Aktel, 2003: 239).

İnternet kavramının ülkeye dahil olmasının 1993 yılına tekabül ettiği Türkiye' de (Yıldız, 2003: 311) 2019 yılı itibariyle nüfusun %94,9' luk dilimi internet, %96,7' lik dilimi ise bilgisayar kullanmaktadır (TÜİK, 2020a). Ancak bilgisayar ve internet kullanımına ilişkin oranlar bu kadar fazlayken, 2018 yılı itibariyle GSYH içerisinde sadece %1,03' lük bir dilim Ar-Ge harcamaları için ayrılmıştır (TÜİK, 2020a). Çalışmanın önceki bölümlerinde bahsedildiği üzere bilgi toplumu içerisinde nitelikli insan faktörünün önemi göz ardı edilemeyecek bir olgudur. Ancak Türkiye' de bilim ve teknoloji alanında yüksek öğretime sahip insan oranı 2019 yılı itibariyle aktif nüfusun %30,3' lük bir dilimini kapsamaktadır (Eurostat, 2020).

Üretim, ekonomi, sosyal yaşam gibi tüm alanlar ve bu alanlarda geçirilen aşamaların temeli bilgiye dayanmalıdır (Saran, 2015). Hem sanayileşme devrini hem de teknolojik gelişimini kendi üretim imkanları dahilinde değil dışarıdan aldığı destekle gerçekleştiren Türkiye, bilgi toplumu olgusunun gerekliliklerini tam anlamıyla yerine getirememektedir (Çukurçayır ve Çelebi, 2012: 77). OECD tarafından sunulan, "İşletmelerde Bilgi ve İletişim Teknolojileri Erişimi ve Kullanımı" istatistikleri 2019 verilerine göre Türkiye'de %51,51' lik bir dilim bu imkanlardan yararlanabilmektedir (OECD,2020). Verilen bilgiler ışığında Türkiye'nin hem yeterli üretim kapasitesine sahip olmadığı hem de ithal ettiği teknolojiyi de işletmeler temelinde yeterince aktif kullanamadığı söylenebilir.

Yenilik temelli oluşan bilgi toplumunda, bütçe içerisinden Ar-Ge faaliyetlerine ve bilgi toplumu olmanın en temel koşullarından birisi olan teknoloji alanına yatırımın arttırılması gerekmektedir (Aktaş, 2007: 191). Bu duruma ek olarak, nitelikli personel hedefi ışığında gerekli eğitimlere önem vermeli, insan ve bilgi odaklı çalışmalar sürdürmelidir (Kocacık, 2003: 9). Bilgi

toplumu düzeyine erişme hedefindeki Türkiye, halihazırda sanayi toplumunun gerekliliklerini de tam anlamıyla yerine getiremediği için alan nezdinde politikalar tasarlayarak küreselleşme olgusu ve beraberinde getirmiş olduğu sürece adapte olmaya çalışmalıdır (Aktan ve Tunç, 1998: 133).

Hem bireylerin hem de kurumların sahip olduğu teknolojik gereçler sayesinde iletişim kavramı, başta internet olmak üzere diğer bileşenleri de içine alarak ulus boyutundan çıkıp ulus ötesi bir görünüm kazanmıştır (Yalçınkaya ve Özsoy, 2003: 6). Bilgi temelinde oluşan, teknoloji, hız, bilişim gibi kavramları hayatımıza dahil eden bilgi toplumu olgusu bu nedenlerle, güvenlik kavramının öneminin anlaşılmasında da büyük rol oynamıştır (Koçak ve Memiş, 2018: 1). Bu noktada sahip olunan bilgi ve iletişim temelli oluşum ve sistemler, muhtemel zararlara karşı hassasiyetle korunmalıdır (Vural ve Sağıroğlu, 2008: 3). Türkiye kapsamında, bahsedilen bilinç ve farkındalık düzeyine erişilip erişilemediği ise çalışmanın bir sonraki bölümünde ele alınmıştır.

III. Türkiye'de Siber Güvenlik Politikaları, Uygulamaları ve Alınan Önlemler

Siber güvenlik kavramının tanımı, önemi, dikkat edilmemesi halinde oluşabilecek maddi manevi kayıplar çalışmanın önceki bölümlerinde bahsedilmiştir. Hal böyleyken Türkiye kapsamında alınan tedbirler ve kavramın yasal dayanaklarına değinmekte yarar vardır. Bilgi toplumu düzeninin gereklilikleri ve yaşanan dijitalleşme süreci, geleneksel güvenlik önlemlerinin de revize edilmesi gerekliliğini ortaya koymuştur (Coşkun ve Yıldırım, 2019: 1560). Bu noktada güvenlik önemleri hakkında nihai söz söyleme yetkisi sadece hükümet esaslı olmamalı, özel sektör ve sivil toplum kuruluşları gibi oluşumların iş birliğine dayanmalıdır (Eryılmaz, 2001: 28).

Siber güvenlik ile ilgili dolaylı olarak birçok kanun düzenlenmiştir. Gelişen teknoloji ve artan bilgi güvenliği ihtiyacı Türkiye'de de gündeme gelmiş, 2003'te başlayan "Dünya Bilgi Toplumu Zirvesi" çalışmaları titizlikle incelenmeye başlanmıştır (Şener ve Erdikmen, 2019: 130-131). Bu bağlamda oluşturulan 5070 sayılı "*Elektronik İmza Kanunu*", 5809 sayılı "*Elektronik Haberleşme Kanunu*" ve ek olarak 5237 sayılı "*Türk Ceza Kanunu"* bilişim suçları, bilgi güvenliği ve siber güvenlik ile ilgili atılan önemli adımlardandır (Coşkun ve Yıldırım, 2019: 1560). 5651 sayılı "*İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi*" hakkındaki kanunun çıkması ile siber suçlar ile mücadele edilmesi adına bir gelişme yaşanmıştır (Kılınç, 2016: 584).

Türkiye'de 2012 yılına kadar siber suçlarla mücadele kapsamında yetkili kurum olan TÜBİTAK, Bakanlar Kurulunun 2012/3842 sayılı "*Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar*" ile yetkisini Ulaştırma, Denizcilik ve

Haberleşme Bakanlığı'na devretmiştir (Şentürk vd., 2012; Aktaran: Bıçakçı vd., 2015: 9). Söz konusu karar uyarınca "Siber Güvenlik Kurulu" kurulmuş ve bakanlık bünyesine bilgi güvenliğini ve gerekli altyapı hizmetlerini korumak, alanda istihdam edilecek personelin donanım kazandırılmasını sağlamak, milli üretimi desteklemek gibi sorumluluklar yüklenmiştir (Bakanlar Kurulu Kararı, 2012). Oluşturulan "Siber Güvenlik Kurulu", "2018/3 Sayılı Cumhurbaşkanlığı Genelgesi" ile kaldırılarak, görevleri Cumhurbaşkanı'na devredilmiştir (2018/3 Sayılı Cumhurbaşkanlığı Genelgesi, 2018).

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı çatısı altında oluşturulan "*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"* ile "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" ve "Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME)" oluşturulması tasarlanmış, gerekli yasal düzenlemeler ile siber güvenlik hususundaki eksikliklerin giderilmesi amaçlanmış, nitelikli insan faktörü göz önünde bulundurularak yerli yazılım ve donanımın geliştirilmesi, altyapının iyileştirilmesi gibi hedefler çerçevesinde siber güvenliğin sağlanıp saldırıların önüne geçilmesi planlanmıştır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013-2014: 17-21). Bir sonraki adım olarak nitelendirilebilecek, 73 kurum ve kuruluş içerisinden toplam 126 uzmanın katılımı doğrultusunda, Ortak Akıl Platformu perspektifinde ülkemizin siber güvenlik alanında atması gereken adımlar, stratejiler belirlendiği "*2016-2019 Ulusal Siber Güvenlik Stratejisi*" oluşturulmuştur (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019: 6). Ulus bazında, siber uzay olarak nitelendirilen boyuttaki tüm paydaşları içine dahil eden bu plan, siber güvenlik alanında gerekli önlemlerin alınması ve bilgi güvenliği ilkelerinin korunması adına atılan eylemler bütünü olma özelliğini göstermektedir (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016-2019: 9).

Telekomünikasyon İletişim Başkanlığı (TİB) çatısında yapılanan "USOM" siber güvenliğin sağlanması adına hem ulusal hem de uluslararası arenayı da kapsayan bağlantı merkezi olma niteliği taşır (Bilgi Teknolojileri ve İletişim Kurumu, 2019). "SOME" ise siber saldırılar ile mücadele kapsamında kurumsal nitelikte yapılanan ve gerekli olduğu taktirde ilgili diğer yapılanmaları konu hakkında aydınlatabilecek kuruluş olma özelliği taşımaktadır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013-2014: 19). Bu oluşumların yanı sıra TÜBİTAK bünyesinde oluşum gösteren "Bilişim ve Bilgi Güvenliği İleri Araştırmalar Merkezi" (Sanalp, 2016: 40), "TSK Siber Savunma Komutanlığı" (Yalçın, 2019: 94), EGM çatısında oluşturulan "Siber Suçlarla Mücadele Daire Başkanlığı" da siber güvenliğin sağlanması hususunda yararlanılan kurumlardandır (Bıçakçı vd., 2015: 36). Tüm bu yapılanmaların, konulan hedeflerin, hayata geçirilen planların yeterli düzeyde olmadığı ise 2017 senesinde yapılan ulusal siber savunma tatbikatı ile açığa çıkmış, tedbirlerin iyileştirilmesi ve siber savunma alanının güçlendirilmesi gerekliliği olgusu ortaya konmuştur (Bıçakçı, 2013: 45-46).

Gelinen son nokta olan, Cumhurbaşkanlığı Hükümet Sistemi'ne geçiş ile birlikte yapılanma gösteren ve Kamu Dijital Dönüşüm Liderini kendine başkan edinen "Dijital Dönüşüm Ofisi" ile,

bilginin her ortamda titizlikle korunmasını sağlayacak projeler geliştirilmesi hedeflenmiştir. İlgili mevzuatta, muhtemel saldırılara karşı tedbirler alınması ve özellikle milli yazılım ve ürünler geliştirilmesi gerekliliği ile güvenliğin önemi vurgulanmaktadır. Ayrıca ofisin, siber güvenlik konusu ile ilgili gerekli kurumlara ilgili önerilerde bulunarak uygulanacak olan faaliyetlerde çalışmalara öncülük etmek gibi bir sorumluluğu vardır (Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, 2018).

Dokuz birimi bünyesinde bulunduran ofisin birimleri ise şu şekildedir:

Şekil 4: Dijital Dönüşüm Ofisi Hizmet Birimleri

Kaynak 4: Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi (2018).

Verilen bilgiler ışığında, siber güvenlik alanı ile ilgili milli teknolojik yapıların geliştirilmesi hedefinin her dönem güncelliğini koruduğu söylenebilir. Bu durumun önemi kapsamında, ABD, Rusya, Çin, Hindistan, İsrail gibi siber güvenlik alanında lider olma istekleri ile gündeme gelmiş ülkelerin, kendi yazılımlarının ve programlarının üretilmesi adına yapılan Ar-Ge çalışmalarını destekleyeceklerini dile getirmeleri ele alınabilir (Kotik, 2015: 69-70). Estonya ve İran örneklerinde de görüldüğü gibi siber saldırılar ciddi oranda maddi ve manevi kayıplara yol açmıştır ve ülkelerde siber güvenlik konusundaki hassasiyet giderek artmıştır (Tatar vd., 2014: 211).

Siber güvenlik alanı ile ilgili önem arz eden yasaların görünürlük kazanmaması ve ilgili kurumlarda alanda nitelikli ve bilinçli insan faktörünün azalması Türkiye'de siber güvenlik alanının gelişmemesinin başlıca nedenleri arasındadır (Bıçakçı, 2015: 61). Ayrıca faaliyetlerin bakanlık bünyesindeki alt alanlar içerisinde değil, ayrı bir oluşum olarak görünürlük kazanması gerekmektedir (Sanalp, 2016: 50). Ülkelerin siber güvenlik güç kapasitelerine önemli bir dayanak olan ve bu alanda gelişim seviyelerini gösteren *"GCI (Küresel Siber Güvenlik Endeksi)"* 2017 verilerine göre Türkiye

164 ülke arasında 43.sırada (ITU, 2017: 60), 2018 verilerine göre ise 175 ülke arasında 20.sırada yer almaktadır (ITU, 2018: 62). Bu veriler ışığında, Türkiye'nin henüz ilk sıralarda yerini almamış olmasına istinaden, siber güvenlik alanında öncü ülke konumunda olmadığı ancak aşama kaydederek ilerlediği iddia edilebilir. Durum, kaydedilen bu aşama ile sınırlı kalmamalı, siber güvenlik hususu ile ilgili bilincin, eğitimin belirli kademelerine kadar indirilip bireylere aşılanması, milli yazılımlarla bilgi güvenliğinin korunması hatta bu durumun ötesine geçilip ilgili yazılım programları ile küresel düzeyde yer edinerek ekonomik fayda sağlanması gerekmektedir (Kotik, 2015: 70). Burada ise tüm sorumluluk devlete düşmemekte, bireyler, özel ve kamusal nitelikteki tüm kurum ve kuruluşlar birlikte çalışmalı ve gerekli faaliyetlerde bulunmalıdır (Yalçın, 2019: 96).

SONUÇ

Bir süreç tarihi olan insanlık tarihi belli dönemlerden geçerek bilgi toplumu seviyesine ulaşmıştır. Bu geçiş aşamasında ise fiziksel güç ve paraya dayalı sermaye yerini beyin gücü ve bilgiye dayalı sermayeye bırakırken, hiyerarşiye dayalı yönetim yapısı da yönetişim temelinde oluşmaya başlamıştır (Kutlu ve Taban, 2007: 15-21). Gelinen nokta olan bilgi toplumu seviyesi ise bilginin en önemli güç unsuru haline geldiği bir toplum düzeni olarak karşımıza çıkmaktadır (Aktan ve Vural, 2016: 3). Bu noktada bilginin üretilmesi, kullanılması, işlenmesi gibi olguların geçerlilik düzeyini koruması ve günden güne gelişimini arttırması, bir ülkenin küresel ölçekteki rakipleriyle rekabet edebilir hale gelmesine olanak sağlamıştır (Aktel, 2003: 239).

Ancak çalışma içerisindeki ilgili literatüre dayanarak varılan sonuç, Türkiye'nin bilgi toplumu seviyesine henüz erişemediği yönündedir. Türkiye' de bilgisayar ve internet kullanımı oldukça fazla olmasına rağmen Ar-Ge harcamaları için ayrılan bütçe çok düşük bir düzeydedir (TÜİK, 2020a). Sadece bilgisayar ve internet kullanımının bilgi toplumu kavramı ile eş değer olmadığı *"Bilgi toplumunu yakalamış olmak tek başına bilgisayar kullanımının belli bir düzeye gelmiş olması ve ağ teknolojilerinin günlük hayatta yaygın bir biçimde yer almasıyla sınırlı değildir"* (Saran, 2015) sözü ile geçerliliğini korumuştur. Eğitimin, nitelikli insan faktörünün oldukça önem kazandığı toplum düzeninde (Kocacık, 2003: 9), Türkiye' de bilim ve teknoloji alanında nitelik kazanmış insan oranı nüfusa oranla düşük bir seyir izlemektedir (Eurostat, 2020). Bu düzeye erişebilmek adına yeni politikalar geliştirmeli (Bozkurt, 2000: 214), alanın temel taşı niteliğinde olan teknoloji alanına, Ar-Ge faaliyetlerine ve insan faktörüne yatırım yapması gerekmektedir (Aktaş, 2007: 191).

Bilgi kavramı ve beraberinde getirdiği toplum düzeni bu kadar önemli bir çizgide ilerlerken, bilgi güvenliği de üzerinde hassasiyetle çalışılması gereken bir konu haline dönüşmüştür (Koçak ve Memiş, 2018: 1). Gelişen teknoloji ve yaygınlaşan internet kullanımı sonucunda karşımıza çıkan kavram ise siber güvenlik olmuştur (Choucri, 2012: 5; Aktaran: Tarhan, 2017: 5). "*Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır"* sözü ile bilgi güvenliği ve siber

güvenlik kavramlarının önemi ve değeri gözler önüne serilmiştir (Nato Güvenlik Danışmanı- Rex Hughes). Yaşanan/yaşanması muhtemel siber saldırılarla bilgi çalınabilir, kötüye kullanılabilir, yetkisiz kişileri eline geçebilir, değiştirilebilir bir unsura dönüşmüştür (Rittinghouse ve Hancock, 2003: 334). Bu doğrultuda hükümetler ilgili tedbirlerin alınması yönünde adımlar atmış ve faaliyetlerde bulunmuşlardır (Önen ve Kurnaz, 2017: 733).

Türkiye kapsamında bilgi güvenliği ve siber güvenlik alanı ile ilgili gerekli maddi, beşerî ve sosyal sermayeye sahip olunmadığı görülmektedir (Yılmaz vd., 2015: 145). Her ne kadar eylem planları geliştirilse, önemli yapılanmalar oluşturulsa da alanda uzman ve yeterli teknik donanıma sahip insan kaynağının olmadığı yapılan siber güvenlik tatbikatında ortaya çıkmıştır (Bıçakçı, 2013: 45-46). Bu doğrultuda, yerli yazılımların ve bilişim sistemlerinin üretilmesi ve kullanılması, yönetişim esaslı uygulama ve kararlar oluşturulması, geçmiş saldırılardan ders alınarak daha güçlü sistemler oluşturulması, zararın sadece dış kaynaklardan değil iç kaynaklardan da gelebileceğinin bilincinde olarak kurum içi personele ilgili güvenlik eğitimlerin verilmesi aracılığı ile siber güvenlik olgusunun gereklilikleri tam anlamıyla yerine getirilmelidir (Yalçın, 2019: 96-97).

KAYNAKÇA

2018/3 Sayılı Cumhurbaşkanlığı Genelgesi (2018) Resmî Gazete (Sayı: 30497), https://www.resmigazete.gov.tr/eskiler/2018/08/20180802.htm, Erişim Tarihi/Access Date: 22.05.2020.

AA (2012), İsrail Ordusu Siber Savaşı Kaybetti, https://www.aa.com.tr/tr/dunya/israil-ordusu-siber-savasi-kaybetti/307287, Erişim Tarihi/Access Date: 21.05.2020.

Aktan, C. C.; Tunç, M. (1998) "Bilgi Toplumu ve Türkiye", Yeni Türkiye Dergisi, 4(19), s. 118-134.

Aktan, C. C.; Vural, İ. Y. (2016) "Bilgi Toplumu, Yeni Temel Teknolojiler ve Yeni Ekonomi", Yeni Türkiye (Bilim ve Teknoloji Özel Sayısı), 1(88), s. 1-37.

Aktaş, C. (2007) "Enformasyon Toplumu Bağlamında Türkiye", Selçuk İletişim, 4(4), s. 181-193.

Aktel, M (2003) Küreselleşme ve Türk Kamu Yönetimi, Ankara: Asil Yayın Dağıtım.

Akyazı, U. (2013) "Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, (Eylül 20-21, Ankara), s. 216-220.

Alavi, M.; Leidner, D. E. (2001) "Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues", MIS quarterly, 25(1), s. 107-136.

Aldemir C.; Şen, E. (2019) "Türkiye'nin Ulusal Siber Güvenlik Stratejisinde Siber Güvenlik Yönetişimi", 13.Uluslararası Kamu Yönetimi Sempozyumu (KAYSEM13), (Nisan 18-20, Gaziantep), s. 1566-1576.

Alpaslan, S.; Kutanis, R. (2007) "Sanayi ve Bilgi Toplumu Yönetim Metaforlarının Karşılaştırılması", Akademik İncelemeler Dergisi (AID), 2(2), s. 49-71.

Arklan, Ü.; Taşdemir, E. (2008) "Bilgi Toplumu ve İletişim: Bilginin Yayılması Sürecinde Kitle İletişim Araçları ve İnternet", Selçuk İletişim, 5(3), s. 67-80.

Aslay, F. (2017) "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", International Journal of Multidisciplinary Studies and Innovative Technologies, 1(1), s. 24-28.

Bakanlar Kurulu Kararı (2012) Resmî Gazete (Sayı: 3842), https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm, Erişim Tarihi/Access Date: 22.05.2020.

Balay, R. (2004) "Küreselleşme, Bilgi toplumu ve Eğitim", Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi, 37(2), s. 61-82.

Baykara, M.; Daş, R. & Karadoğan, İ. (2013) "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", 1st International Symposium on Digital Forensics and Security (ISDFS'13), (Mayıs 20-21, Elazığ), s. 231-244.

Bedir, E. (2002) "Yirmibirinci Yüzyılda İstihdamın Artan Önemi ve Eğitim-İstihdam İlişkisi", Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 4(2), s. 53-64.

Bell, D. (2013) İdeolojinin Sonu: Ellilerdeki Siyasi Fikirlerin Tükenişine Dair (Çev.) Volkan Hacıoğlu, Bursa: Sentez Yayıncılık.

Bıçakçı S. (2012) "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", Uluslararası İlişkiler Dergisi, 9(34), s. 205-226.

Bıçakçı, S. (2013) 21. Yüzyılda Siber Güvenlik, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Bıçakçı, S.; Ergun, D. & Çelikpala, M. (2015) "Türkiye'de Siber Güvenlik", Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi, (1), s. 1-35.

Bilgi Teknolojileri ve İletişim Kurumu (2019), USOM ve Kurumsal Siber Olaylara müdahale, https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Erişim tarihi/Access Date: 18.12.2019.

Bilgi Toplumuna Dönüşüm Politika Belgesi (2005), http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Bilgi_Toplumuna_Donusum_Politika_Belgesi_2005.pdf, Erişim Tarihi/Access Date: 20.05.2020.

Bozkurt, V. (2000) Enformasyon Toplumu ve Türkiye (3. Baskı), İstanbul: Sistem Yayıncılık.

Coşkun, B.; Yıldırım, Ç. P. (2019) "Kolluk Hizmetinden Siber Güvenliğe: Güvenlik Yönetiminde Değişim", 13.Uluslararası Kamu Yönetimi Sempozyumu (KAYSEM13), (Nisan 18-20, Gaziantep), s. 1555-1566.

Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi (2018). Resmî Gazete (Sayı: 30474), https://www.mevzuat.gov.tr/MevzuatMetin/19.5.1.pdf, Erişim Tarihi/Access Date: 19.12.2019.

Çalık, D.; Çınar, Ö, P. (2009) "Geçmişten Günümüze Bilgi Yaklaşımları Bilgi Toplumu ve İnternet", XIV. Türkiye'de İnternet Konferansı (Aralık 12-13, İstanbul), s. 77-88.

Çifçi, H. (2013) Her Yönüyle Siber Savaş, Ankara: TÜBİTAK Popüler Bilim Kitapları

Çukurçayir, M. A.; Çelebi, E. (2012) "Bilgi Toplumu ve E-devletleşme Sürecinde Türkiye", Uluslararası Yönetim İktisat ve İşletme Dergisi, 5(9), s. 59-82.

Doherty, N. F.; Anastasakis, L. & Fulford, H. (2009) "The Information Security Policy Unpacked: A Critical Study of the Content of University Policies", International Journal of Information Management, 29(6), ss. 449-457.

Drucker, P. F. (1994) Yeni Gerçekler (Çev.) Birtane Karanakçı, Ankara: Türkiye İş Bankası Kültür Yayınları.

Durna, U.; Demirel, Y. (2008) "Bilgi Yönetiminde Bilgiyi Anlamak", Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, (30), s. 129-156.

Eminağaoğlu, M.; Gökşen, Y. (2009) "Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri", Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11(4), s. 1-15.

Erkan, H. (1994). Bilgi toplumu ve Ekonomik Gelişme, İstanbul: Türk İş Bankası Yayını.

Erkan, H. (1998) "21. Yüzyıla Girerken Bilgi Toplumu ve Türkiye", Yeni Türkiye Dergisi, 4(19), s. 134-143.

Erkan, H. (2004) Ekonomi Sosyolojisi 5.Baskı, İzmir: Barış Yayınları.

Eryılmaz, B. (2001) Kamu Yönetimi, İstanbul: Erkam Matbaası.

Eurostat (2020), Human Resources in Science and Technology (HRST), https://ec.europa.eu/eurostat/databrowser/view/tsc00025/default/table?lang=en, Erişim Tarihi/Access Date: 22.05.2020.

Ezer, M. (2018) "Türkiye'de Bilgi Toplumunun Gelişimi: Kişisel İnternet Kullanım Amaçları Üzerine Bir Uygulama (Tez No: 497948) [Yayımlanmamış Yüksek Lisans Tezi], Çukurova Üniversitesi, Sosyal Bilimler Enstitüsü.

Fındıkçı, İ. (1997) Bilgi Toplumunda Yöneticilerde Kendini Geliştirme, İstanbul: Kültür Koleji Eğitim Vakfı Yayınları.

International Telecommunication Union (ITU) (2017), Global Cybersecurity Index, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf, Erişim Tarihi: Access Date: 25.05.2020

International Telecommunication Union (ITU) (2018), Global Cybersecurity Index, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, Erişim Tarihi: Access Date: 25.05.2020

Hekim, H.; Başıbüyük, O. (2013) "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), s. 135-158.

İşbilen, F. M. (2016) "Bilgi Toplumuna Geçiş Sürecinde Türkiye" (Tez No: 448668) [Yayımlanmamış Yüksek Lisans Tezi], Kırıkkale Üniversitesi, Sosyal Bilimler Enstitüsü.

Kamu Bilgi ve İletişim Teknolojileri Yatırımları (2019), http://www.bilgitoplumu.gov.tr/wp-content/uploads/2019/08/Kamu_bit_yatirimlari_2019.pdf, Erişim Tarihi: Access Date: 22.05.2020.

Keleş, A. R.; Sal, Y. (2013) Hack Kültürü ve Hacktivizm: Yeni Bir Siyaset Biçimi, İstanbul: Alternatif Bilişim Derneği Yayınevi.

Kitchin, R. (2014) The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences, London: Sage.

Kara, M. (2013) "Siber Saldırılar-Siber Savaşlar ve Etkileri", [Yayımlanmamış Yüksek Lisans Tezi], İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, https://afyonluoglu.org/PublicWebFiles/Reports-TR/Akademi/2013-TEZ-Siber%20Sald%C4%B1r%C4%B1lar%20Siber%20Sava%C5%9Flar%20ve%20Etkileri.pdf.

Kılınç, D. (2016) "5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A Maddesi Çerçevesinde Özel Hayatın Korunması", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 20(2), s. 577-624.

Kocacık, F. (2003) "Bilgi toplumu ve Türkiye", CÜ Sosyal Bilimler Dergisi, 27(1), s. 1-10.

Koçak, H.; Memiş, K. (2018) Bilgi Toplumunda Korku: Bilgi Güvenliği ve Risk Toplumu, Afyon Kocatepe University Journal of Social Sciences, 20(3), s. 1-10.

Kotik, Ö. Y. (2015) "Uluslararası İlişkilerde Siber Güvenlik Algısı ve Ulus Devletin Değişen Stratejisi" (Tez No: 417580) [Yayımlanmamış Yüksek Lisans Tezi], Çukurova Üniversitesi Sosyal Bilimler Enstitüsü.

Kutlu, E.; Taban, S. (2007) Bilgi Toplumu ve Türkiye, Ankara: Pelikan Yayınevi.

Langner, R. (2011) "Stuxnet: Dissecting a Cyberwarfare Weapon", IEEE Security & Privacy, 9(3), s. 49-51.

Libicki, M. C. (2009) Cyberdeterrence and Cyberwar, Santa Monica: Rand Corporation.

Mayor, T. (2013) "Avcı-toplayıcılar: Orijinal Liberteryenler" (Çev.) Atilla Yayla, Liberal Düşünce, (71), s. 227-246.

Organisation for Economic Co-operation and Development (OECD) (2020), ICT Access and Usage by Businesses, https://stats.oecd.org/, Erişim Tarihi/Access Date: 22.05.2020.

Orkan, A.L. (1992) "Bilişime Teorik Yaklaşım ve Bazı Temel Kavramlar", Marmara İletişim Dergisi, (1), s. 93-108.

Öğün, M.N.; Adem, K. (2013) "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", Güvenlik Stratejileri Dergisi, 9(18), s. 145-181.

Önen, S.M.; Kurnaz, S. (2017) "Siber Güvenlik Politikalarının Kamu Yönetimine Yansıması", Turgut Özal Uluslararası Ekonomi ve Siyaset Kongresi IV (Mayıs 11-12, Malatya), s. 732-753.

Özdemir, Ş. (2014) "Sanayi Devriminin Bilim Tarihi Üzerindeki Etkisi: Bilim ve Teknoloji İç İçe", Üretim Ekonomisi Kongresi, (Mart 21-22, İstanbul), s. 1-11.

Özdemirci, F.; Torunlar, M. (2018) "Bilgi-Değişim-Siber Güvenlik-Bağımsızlık", Bilgi Yönetimi, 1(1), s. 78-83.

Özsağır, A. (2013) Bilgi Ekonomisi: Tanım-Uygulamalar-Örnekler, Ankara: Seçkin Yayınevi.

Peltier, T. R. (2005) "Implementing an Information Security Awareness Program", Information Systems Security, 14(2), s. 37-49.

Rittinghouse, J.; Hancock, W. M. & Cissp, C. (2003) Cybersecurity Operations Handbook, USA: Digital Press.

Saltzer, J. H.; Schroeder, M. D. (1975) "The Protection of Information in Computer Systems", Proceedings of the IEEE, 63(9), s. 1278-1308.

Sanalp, S. (2016) "Çeşitli Ülkelerde USOM ve SOME Yapılandırılması ve Türkiye Modeli Önerisi" (Tez No: 431496) [Yayımlanmamış Yüksek Lisans Tezi], İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü.

Saran, U. (2015), Türkiye Bilgi Toplumu Olmaya Ne Kadar Yakın? http://www.aljazeera.com.tr/gorus/turkiye-bilgi-toplumu-olmaya-ne-kadar-yakin, Erişim Tarihi/Access Date: 23.05.2020.

Şanlısoy, S. (1999) "Bilgi Toplumunda Ortaya Çıkabilecek Sorunlar", Dokuz Eylül Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi, 14(2), s. 169-194.

Şener, G.; Erdikmen, A. (2019) "Yeni Medya Çalışmaları V: Türkiye İnternet Tarihi", iç. Türkiye'de Erken Dönem İnternet Aktivizmi, (Ed.) Erkan Saka, İstanbul: Alternatif Bilişim Derneği Yayınevi. s. 129-184.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Bilgi ve İletişim Teknolojileri Dairesi (2020), http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/, Erişim Tarihi/Access Date: 20.05.2020.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2013-2014), Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, Erişim Tarihi/Access Date: 22.12.2019.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016-2019), 2016-2019 Ulusal Siber Güvenlik Stratejisi, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, Erişim Tarihi/Access Date: 23.12.2019.

Tarhan, K. (2017) "Siber Uzayda Realist Teorinin Değerlendirilmesi", Cyberpolıtık Journel, 2(3), s. 1-17.

Tatar, Ü.; Çalık, O.; Çelik, M. & Karabacak, B. A. (2014) "A Comparative Analysis of the National Cyber Security Strategies of Leading Nations", Proceedings of the 9th International Conference on Cyber Warfare and Security (March 24-25, West Lafayette, Indiana, USA), s. 211-218.

Tekerek, M. (2008) "Bilgi Güvenliği Yönetimi", KSÜ Fen ve Mühendislik Dergisi, 11(1), s. 132-137.

Türkiye İstatistik Kurumu (TÜİK) (2020a), Bilgi Toplumu İstatistikleri, 2004-2019, http://www.tuik.gov.tr/UstMenu.do?metod=temelist, Erişim Tarihi/Access Date: 22.05.2020.

Türkiye İstatistik Kurumu (TÜİK) (2020b), E-devlet Kalkınma Endeksi, http://www.tuik.gov.tr/UstMenu.do?metod=istendeks, Erişim Tarihi/Access Date: 24.05.2020.

Türkiye İstatistik Kurumu (TÜİK) (2020c), Bilgi ve İletişim Teknolojileri Gelişmişlik Endeksi, http://www.tuik.gov.tr/UstMenu.do?metod=istendeks, Erişim Tarihi/Access Date: 24.05.2020.

Uçak, N. Ö. (2010) "Bilgi: Çok Yüzlü Bir Kavram", Türk Kütüphaneciliği, 24(4), s. 705-722.

Ulusoy, A.; Karakurt, B. (2002) "Türkiye'nin E-Devlete Geçiş Zorunluluğu", I. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi, (Mayıs 10-11, İzmit), s. 131-144.

Ulusoy, A.; Karakurt, B. (2002) "Türkiye'nin E-Devlete Geçiş Zorunluluğu", I. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi, (Mayıs 10-11, İzmit), s. 131-144.

Vural, Y.; Sağıroğlu, Ş. (2008) "Ülke Bilgi Güvenliği", 3.Uluslararası Katılımlı Bilgi güvenliği ve Kriptoloji Konferansı (Aralık 25-27, Ankara), s. 3-20.

Yalçın, İ. (2019) "Soğuk Savaş Sonrası NATO ve Türkiye'de Siber Güvenlik" (Tez No: 545623) [Yayımlanmamış Yüksek Lisans Tezi], Eskişehir Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü.

Yalçınkaya, T.; Özsoy, E. (2003) "Risk Toplumu: Bilgi Toplumunun Evriminde Yeni Boyut", II. Uluslararası Bilgi, Ekonomi ve Yönetim Kongresi, (Mayıs 17-18, İzmit), s. 1-10.

Yıldız, M. (2003) "Elektronik E-Devlet Kuram ve Uygulamasına Genel Bir Bakış ve Değerlendirme", iç. Çağdaş Kamu Yönetimi- I, (Ed.) Muhittin Acar, Hüseyin Özgür, Ankara: Nobel Yayın Dağıtım, s. 305-327.

Yılmaz, B. (2013) "E-dönüşüm Sistemlerinin Bilgi Güvenliği Açısından İncelenmesi E-devlet Kullanıcıları Üzerine Bir Araştırma (Tez No: 327359) [Yayımlanmamış Yüksek Lisans Tezi], Marmara Üniversitesi. Sosyal Bilimler Enstitüsü.

Yılmaz, E.N.; Ulus, H.İ. & Gönen, S. (2015) "Bilgi Toplumuna Geçiş ve Siber Güvenlik", Bilişim Teknolojileri Dergisi, 8(3), s. 133-146.

Yılmaz, M. (2009) "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi", Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, 49(1), s. 95-118.

Yılmaz, T (2006) "Bilgi Toplumuna Geçiş Sürecinin Türkiye'de Finansal Piyasalar Üzerindeki Etkisi" (Tez No: 189714) [Yayımlanmamış Yüksek Lisans Tezi], Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü.