Bilgi Toplumuna Geçiş ve Siber Güvenlik

Ercan Nurcan YILMAZ, Halil İbrahim ULUS, Serkan GÖNEN

Gazi Üniversitesi Teknoloji Fakültesi Elektrik Elektronik Mühendisliği Bölümü
enyilmaz@gazi.edu.tr, halilulus@gmail.com, serkangonen@gmail.com
(Geliş/Received: 20.03.2015; Kabul/Accepted: 18.08.2015)
DOI: 10.17671/btd.87028

Özet— Bilgi teknolojileri altyapısının gelişmesi ve geniş coğrafi alanlara yayılması bireylerin, toplumların, kurumların ve devletlerin birbirleri ile olan ilişkilerini iletişim ve bilgisayar ağları üzerinden yürütebilmelerine olanak sağlamıştır. Günümüzde yaklaşık 2 milyar insan internet kullanmaktadır ve Microsoft'un araştırmasına göre bu sayının 2025 yılına kadar hızla artarak 4 milyarı geçmesi beklenmektedir. Kullanıcı sayısı arttıkça genel tanımlama ile "Siber Güvenlik" olarak adlandırdığımız problem ortaya çıkmaktadır. Artık ülkeler kendi bilgi sistemlerini ve kritik altyapılarını bilgi teknolojileri altyapısıyla oluşturmaktadır. Ancak, bu sistemlerin korunması için de yine bilgi teknolojileri altyapısı kullanılmakta ve bir kısır döngü oluşmaktadır. Ülkeler siber alana bağımlı olan sistemlerini siber tehditlere karşı korumak için standartlar, politikalar ve stratejiler geliştirmiş ve uygulamıştır. Bu çalışmada teknolojinin gelişmesiyle birlikte küreselleşmeye bağlı güvenlik kaygılarının ortaya çıkışı, ülkemizde uygulanan bilgi toplumu stratejisi, ülkemiz ve dünyada bilgi toplumuna geçiş süreci, bilgi teknolojileriyle oluşturulan kritik altyapı sistemleri, bu sistemlere karşı siber tehditler ve bu sistemlerin risk analizi incelenmiştir.

Anahtar Kelimeler— Siber güvenlik, Bilgi toplumu, Kritik altyapılar

Transition to Information Society and Cyber Security

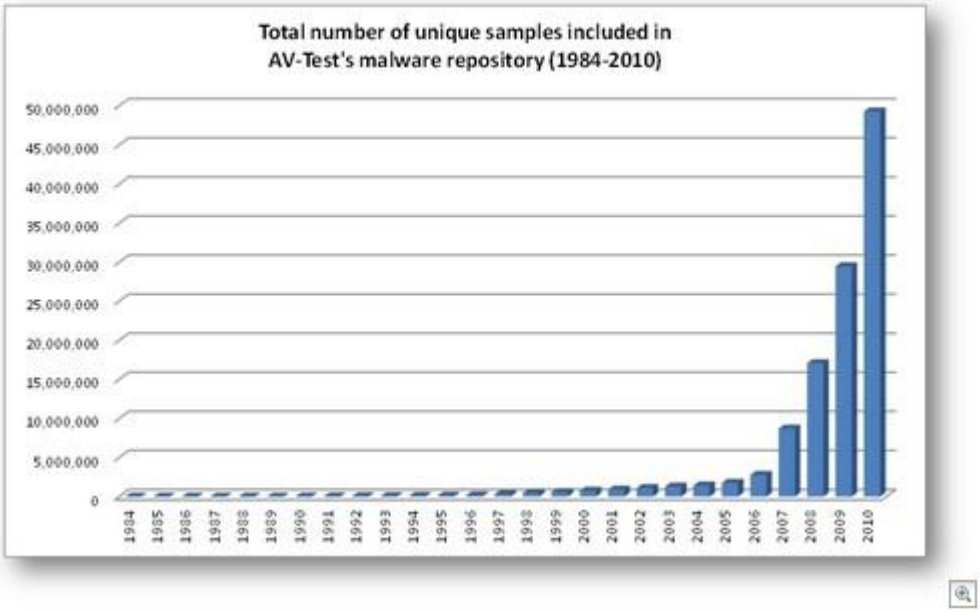
Abstract— Improving of information infrastructure technologies and expanding to broad geographical areas; enable persons, societies, institutions and states communicates with the help of communication and computer networks. Nowadays, approximately 2 billion people use internet and according to Microsoft search, passing to 4 billions is hoped till 2025. With increasing of users quantity, generally of privately "Cyber security" problem comes up. Now countries use information technologies while constituting own information system and critical infrastructure. But for the protection of these systems still in use in information technology infrastructure and there occurs a vicious circle. Countries of the system to protect against cyber threats that are dependent on cyber field, standards, policies and strategies developed and implemented. In this study, the emergence of globalization depends on security concerns with the development of technology, information society strategy applied in our country, the knowledge society transition period in our country and around the world, critical infrastructure created by information technology, cyber threats against the system and risk analysis of these systems examined.

Keywords— cyber security, information society, critical infrastructure.

1. GİRİŞ (INTRODUCTION)

İnsanlık tarihinde evreler farklı bir tekniğin, keşfin ve yöntemin ortaya çıkmasına sahne olmuştur. Özellikle 1900'lü yılların sonuna doğru sıra dışı buluşlar, yenilikler ortaya çıkmıştır. Bunlardan en önemlisi, bugün 2,3 milyar kişinin kullandığı internettir. 1960 yılında internetin ilk kurulma amacı bilgi paylaşmaktı. Bu yüzden, ilerleyen zamanlarda internetin bu denli yaygınlaşacağı beklenmediğinden ve insanların sisteme zarar verebilecekleri düşünülmediğinden güvenlik geri planda bırakılmıştır. Teknolojik gelişmeye paralel olarak altyapıların bilişim sistemlerine bütünleşme çabaları artmış, küreselleşme ve getirdiği iş kolaylığı gibi nedenlerden ötürü bu geçiş hızlanmıştır. Önceleri kritik altyapılara karşı oluşabilecek tehditler fiziksel olarak

değerlendirilirken; zamanla zararlı kodların ortaya çıkması ve bilişim sistemlerine bağımlı hale gelen kritik altyapıları yıllar içinde artan bir oranda tehdit etmesi (Şekil.1), tehlikenin seviyesinde şekil değişikliğine sebep olmuştur [1].



Şekil 1. Zararlı Yazılımların Artışı [2]
(Increase of Malware)

Dünyada ortaya çıkan bu yeni durum ekonomik, siyasal ve sosyal olarak uluslararası alanda yeni bir yapı yani küreselleşmeyi meydana getirmiştir. Küreselleşme; sosyal, kültürel ve siyasal değerlerin, düşüncelerin, birikimlerin ulusal sınırları aşarak dünya geneline yayılması ve uluslararası alanda diğer unsurları etkilemesidir. Bu bağlamda; bilgi teknolojileri her ne kadar küreselleşmeye yön veren aktörler için söz sahibi olma yönünde etkili bir araç olsa da; diğer ülkeler için kaçınılmaz olarak benimsettirilen ve rekabet için takip edilmesi gereken önemli bir yeniliktir [3].

Daha önceki dönemlerde yeni doğal kaynakların, yeni kıtaların, yeni ticaret yollarının keşfedilmesi sonucu ortaya çıkan ekonomik gelişmelerden farklı olarak şimdi, bilgisayar teknolojisi ile yaratılan görünmeyen bir kıta (internet dünyası) keşfedilmiştir. Bu buluş, sadece üretim ve tüketimde değil mekân anlayışında köklü bir değişiklik getirmiş, insanların sosyal ilişkilerinde mekânın zorunluluğunu ortadan kaldırmıştır. Bu yüzden bilgi toplumu ile küreselleşmenin iç içe ve birbirlerinin tamamlayıcı parçaları olduklarını belirtebiliriz. Böylece bilgi teknolojileri ve iletişim sistemleri ile küreselleşme hız kazanmış, ülke sınırları küçülmüş, rekabet ortamı şiddetlenmiş, bölgesel gruplaşmalar başlamış ve bugün için ülkelerin fiziksel alan dâhil tüm etki alanları siber alandaki yetkinliklerine göre sınırlanmıştır [4].

2. BİLGİ TOPLUMUNA GEÇİŞ VE TÜRKİYE (TRANSITION TO INFORMATION SOCIETY)

Ulusal bilgi altyapılarını oluşturan ülkeler, bu doğal süreç içerisinde ülkenin ekonomik açıdan büyümesi ve verimliliğinin artması, yeni iş sahası olanakları, haberleşme ve yazılım teknolojileri avantajları, uluslararası alanda kritik teknolojilerde liderlik sağlanması gibi nedenlerden ötürü bilgi teknolojilerine yatırım yapmaya devam etmektedirler. Bu yüzden rekabet gücünü kaybetmemek adına Türkiye de bilgi ve iletişim teknolojisine ve altyapısına, bu sistemlerin güvenliğine yönelik yatırımlar yapmakta ve çeşitli ulusal boyutta çalışmalar yürütmektedir [5].

Türkiye'nin bilgi toplumuna geçiş için e-sistemlerin kullanımına başlaması, 1960'lı yıllara dayanmaktadır. Buna örnek olarak; Dünya'daki 12 sistemden birisi olan ilk bilgisayar Karayolları Genel Müdürlüğü'nde bulunması verilebilir (30 Ekim 1960). Ayrıca 1963'te DSİ ve İş Bankası'nın bilgisayar sahibi olduğu; İTÜ ve ODTÜ'nün 1964 ve 1965 yıllarında ilk kursları tertip ettiği; 1970'li yılların başında İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünün Merkezi Nüfus İstatistikleri Projesini (MERNİS) başlattığı, 1980'lerin ortasında bilgisayarlar ortaya çıkışında patlama yaşandığı, 1993 yılında ilk defa Orta Doğu Teknik Üniversitesi ve ABD arasında kiralık bir hat üzerinden internet bağlantısı sağlandığı ve 1995'te internetin kullanılmaya başlandığı çeşitli kaynaklardan anlaşılmaktadır [6].

Bu gibi örnekler vererek Türkiye'nin bilgi toplumuna geçiş sürecini çok eskilere dayandırmak mümkün olsa da TBMM'de Bilgi ve Bilgi Teknolojileri Grubunun oluşturulduğu 1998 yılını, bu dönüşümün başlangıcı olarak kabul edebiliriz. Bu tarihten sonra birçok resmi ve gayri resmi toplantılar yapılarak geçiş için altyapı oluşturulmaya çalışılmıştır. Özellikle küreselleşmenin etkisi ve AB uyum paketlerinde belirtilen ilkeler gereği; Türkiye'nin, 2001 yılında AB'ye aday ülkeler için hazırlanan eAvrupa+ girişimine taraf olmasıyla, Türkiye'de bilgi toplumuna dönüşüm faaliyetleri 2000'li yılların başından itibaren hız kazanmaya başlamıştır [6].

Bilgi Toplumuna geçiş çalışmalarıyla birlikte e-devlet ve e-vatandaş kavramları ortaya çıkmış, eskiden manuel olarak yönetilen özel ve kamu altyapıları bilgisayar sistemleri tarafından kontrol ve denetlenmeye başlanmıştır. Özellikle bu alanda hazırlanan e-Dönüşüm Türkiye Projesi kapsamında bu geçiş sürecinin vatandaş, özel sektör ve kamu kurumları arasında uyum içinde ve bütünleşik bir şekilde yürütülmesi amaçlanmıştır. Bu alandaki politika ve kanunların, AB mevzuatı ile birlikte yeniden değerlendirilerek, Avrupa'da hazırlanan eAvrupa+ eylem planına paralel olarak e-Türkiye Girişimi Eylem Planı başlatılmıştır. Bu sayede geleneksel devlet anlayışından farklı olarak Tablo 1'de de görüleceği üzere kamu alanında bilgi ve iletişim sistemlerinin azami ölçüde kullanılması, bu teknoloji yardımıyla kaynak israfının azaltılması, tekrar eden ve örtüşen projelerin birleştirilmesi ve yatırımcı kuruluşlarla koordinasyonun yapılması amaçlanmıştır [7].

Tablo 1. Geleneksel Devlet Anlayışı ile E-devlet Anlayışının Karşılaştırılması [8]
(Comparing with Traditional State Conception and E-Government Conception)

Geleneksel (Klasik) Devlet Anlayışı	**E-Devlet Anlayışı**
Bürokratik Kontroller	Bireye ve topluma hizmetin ön plana çıkması
İzole edilmiş idari fonksiyonlar	Entegre kaynak hizmetleri; açık, şeffaf, sorgulanabilir devlet
Kağıt işi ve dosyalama sistemi	Elektronik hizmet sistemi
Zaman tüketen süreçler	Hızlı, kolay iş süreçleri
Elle düzenlenen finansal sözleşmeler	Elektronik fon transferi ve kontrol
Standart dışı raporlama sistemleri	Bilgiye esnek erişim ve standart işlemler
Bağlantısız, koordinesiz bilgi teknolojileri	Bütünleşmiş ağ çözümü
Yüz yüze işlem zorunluluğu	Uzaktan elektronik işlem imkanı
Her dönem idareci seçimi	Gerçek, katılımcı ve sürekli demokrasi

Müteakiben 2003-2004 yıllarını kapsayan e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı hazırlanmıştır. E-devlet çalışmaları 2006-2010 yılları arasında Bilgi Toplumu Stratejisi ve Eylem Planı gibi kapsamlı bir politikanın içinde yürütülmüştür. Ayrıca Kalkınma Bakanlığınca Türkiye'de e-devlet çalışmalarının da içinde yer aldığı Bilgi Toplumu Stratejisinin ikinci safhası olarak nitelendirilebilecek sekiz ana eksenli Bilgi Toplumu Stratejisi ve Eylem Planı 2014-2018 taslağı hazırlanmış ve kamuoyuna duyurulmuştur [9].

E-devlet; devletin vatandaşlarına karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile vatandaşların devlete karşı olan görev ve hizmetlerinin karşılıklı olarak elektronik iletişim ve işlem ortamlarında kesintisiz ve güvenli olarak yürütülmesidir. Birleşmiş Milletler Örgütü ve Amerika Kamu Yönetimi Derneği tarafından yapılan bir çalışmada ise e-devlet kurulum ve uygulama aşamaları beşe ayrılmıştır:

1. *E-devletin ortaya çıkış aşaması:* (Kurumsal sitelerin ortaya çıkışı)
1. *Gelişme aşaması:* (sitelerin sayısının ve fonksiyonları artması)
2. *İnteraktif aşama:* (Kullanıcıların devlete ait sitelerden ihtiyaç duyduğu belgeleri indirebilmesi)
3. *İşlem aşaması:* (Kullanıcıların bazı hizmetlerin ücretlerini internet sitelerinden ödeyebilmesi)
4. *Kesintisiz bütünleşme* veya sorunsuz olarak kamu idarelerinin internet siteleri ve burada sunulan kamu hizmetlerinin birbirine bağlanması: (e-devlet kapısı) [10].

E-Devlet projesinde amaç devlet hizmetlerinin vatandaşlara kolay, hızlı, kaliteli ve kesintisiz sağlanmasıdır. Günümüzde bunu hızlı ve düşük maliyetle gerçekleştirecek kurumlara ve bunları koordine edecek sistemlere ihtiyaç duyulmaktadır [11]. Bu gerçekleştirecek e-devlet sisteminin uygulanması dört aşamada olacaktır. Bunlar oluşturulan web sayfalarında bilgi sunulması, bazı hizmetlerin çevrimiçi sağlanması, tek bir devlet ana kapısı oluşturarak hizmetlerin tek kaynaktan sunulması ve yeni hizmetlerin ortaya çıkmasıdır. Geleneksel kamu hayatında vatandaşların ya da diğer kurumların iş süreçleri ilgili birimlerle yüz yüze görüşerek dilekçe yazma, form doldurma, evrak tamamlama gibi faaliyetleri içerirken e-devlette elektronik ortamda yapılabilmektedir. Ülkemizdeki e-Devlet oluşumunda yer alan birçok proje bulunmaktadır. Türkiye Ulusal Bilgi Sistemleri içerisinde yer alan ve bilgi güvenlik altyapısı, mesaj sistemi, sayısal haritaları, ara yüzleri, veri bankaları, veri sözlüğü ve işlevleri olan bu projelerden bazıları aşağıda sıralanmıştır [12].

Bu doğrultuda kamu kurumlarında da birçok proje gerçekleştirilmiştir. Merkezi yönetim tarafından yönetilen bu uygulamalar, merkez teşkilatı içinde yer alan çeşitli kurumların bağımsız çabaları sonucu ortaya çıkmıştır. Özellikle en önemlisi 1972 yılında çalışılmaya başlanan ve 2002 yılında hizmete geçen MERNİS (Merkezi Nüfus İdaresi Sistemi) projesidir. Proje ile her vatandaşın işlemleri kimlik numarası sayesinde takip edilebilmektedir. Fakat diğer bakanlıklar tarafından hazırlanan bağımsız uygulamalar ile bir eşgüdüm, bütünleşik ve koordineli bir yapı oluşturulamamıştır. Bu tür diğer uygulama örnekleri aşağıda sıralanmıştır:

- Kamu-Net Projesi: Projenin genel amacı tüm kamu kuruluşlarının veri alışverişini bilgisayar ortamında yapmasını, ortak veri tabanı kullanmalarını ve kâğıt kullanımını azaltarak elektronik ortama geçmek amaçlanmaktadır. 1998 yılında kurulan bu ağ ile vatandaşa verilen hizmetin hızlı ve pratik olarak yapılması hedeflenmektedir.
- VEDOP (Vergi Daireleri Otomasyon Projesi)
- GİMOP (Gümrük İdaresinin Modernizasyonu)
- ULAKBİM (Ulusal Akademik Ağ ve Bilgi Merkezi): Eğitim, araştırma ve geliştirme yapan kişi ve kuruluşlar arasında iletişim sağlamak, yurtiçi ve yurtdışı kaynaklara ulaşmak amacıyla oluşturulmuştur.
- UYAP (Ulusal Yargı Ağı Projesi
- POLNET(Emniyet Bilgi Sistemi
- TAKBİS (Tapu Kadastro Bilgi Sistemi).
- Sağlık Bilgi Sistemi
- Maliye Bakanlığı Bilgi Sistemi (SAY2000)
- Adalet Bakanlığı Bilgi Sistemi
- Eğitim Bilgi Sistemi
- Sosyal Güvenlik Bilgi Sistemi
- Sanayi Bakanlığı e-Tüketici (e-Hizmetler) Projesi, Çalışma ve Sosyal Güvenlik Bakanlığı e-Bildirge ve MEDULA Projeleri
- Milli Savunma Bakanlığı ASAL Projesi, Dışişleri Bakanlığı e-Dışişleri Projesi
- Başbakanlık Bilgi İşlem Merkezi Projesi (BİMER)
- Kimlik Paylaşım Sistemi (KPS) [13].

Yukarıda belirttiğimiz kurumsal bilgi sistemlerinin kurulmasına paralel olarak özellikle 2009-2013 yılları arasında kamu kurumlarının web siteleri kullanım oranı da artmış halkın daha hızlı hizmet alması amaçlanmıştır. Tablo 2' de 2009 ve 2013 yıllarında ülkemizde mevcut web site sayıları gösterilmektedir.

Tablo 2. ODTÜ'de Konuşlu Nic.tr Yönetiminin 2013 Tarihli Araştırma Sonucu
(Based in METU Nic.tr Management dated 2013 Research Results)

	2009	**2013**
gov.tr (hükümet) uzantılı	8766	11901
bel.tr (belediye) uzantılı	2225	2478
edu.tr (üniversite-eğitim) uzantılı	421	538
tsk.tr (silahlı kuvvetler) uzantılı	34	36
mil.tr (askeri kurum ve kuruluşlar tarafından alınabilen alt alan adı)	8	2
pol.tr (emniyet teşkilatı tarafından alınabilen alt alan adı)	309	474
k.12.tr (Milli Eğitim Bakanlığınca onaylanmış ilköğretim, lise ve dengi okullar tarafından alınabilen addır)	9408	10531
TOPLAM	21.171	25.960

E-devlet uygulamalarının en önemli öğelerinden biri kişisel bilgilerin doğru olması ve yapılan işlemlerin güvenli bir ortamda gerçekleştirilmesidir [14]. Oluşturulan güvenlik politikası şu üç özelliğe sahip olmalıdır;

• *Koruma:* Kullanıcılardan toplanılan bilgilerin korunması, bunların kullanılma şekilleri ile yapılan tüm işlemlerin gizli kalması ve dışarı sızdırılmaması gibi prensipleri ihtiva eder.

• *Yeterlilik:* Kullanıcının ulaşmak istediği işlem ile ilgili olarak sadece gerekli bilgileri girmesi, o anki işlemle ilgili olmayan şahsi bilgileri girmek zorunda bırakılmaması durumudur.

• *Güvenlik*: E-devlet uygulamaları üzerinden yapılan tüm işlemlerin veri güvenliğinin sağlanması ve dışarıdan oluşabilecek tüm saldırılara karşı güvenlik duvarlarının ve önlemlerinin oluşturulmasıdır.

Yukarıda saydığımız prensipler ışığında ülkemizde vatandaşlara hizmet veren kamu web siteleri ve bu siteler üzerinden yapılan sorgulama işlemleri incelendiğinde iki önemli nokta ortaya çıkmaktadır:

• İlki; herhangi bir sorgulama işlemi için kullanıcıdan iki ya da üç farklı bilgi istenmekte, fakat sorgulama işlemi sonunda kullanıcıya işlemin amacından çok fazla ayrıntılı bilgi verilmektedir. Böylece kullanıcı istemediği bilgileri de almaktadır.

• İkincisi; herhangi bir sorgulama işleminden elde edilen bilgiler başka bir web uygulamasında sorgu parametresi olarak kullanılabilmektedir. Böylece bir web sitesinden alınan bilgi ya da bilgiler farklı bir web sitesinde kullanılarak yeni bilgilere ulaşılabilmektedir [9].

Bu örnekler göstermektedir ki; yukarıda belirttiğimiz bu süreç çok hızlı gerçekleşmekte, alınan tedbirler oluşabilecek riskleri karşılamada yetersiz kalabilmektedir. Bu geçiş sürecinin iyi yönetilememesi halinde milli sistemlerimize karşı tehditler ortaya çıkabilmektedir. Şekil.2'de e-devlet uygulamalarına karşı güvenlik ihlalleri görülmektedir. Günümüzde e-devlet uygulamalarına yönelik siber tehditler o kadar artmıştır ki siber güvenlik unsurları yetersiz kalmaktadır. Bunun örneklerini yakın zamanda olan TEİAŞ sistemlerine yetkisiz erişim, Ankara'daki vatandaşların tapu bilgilerinin çalınması, HSBC Bankasının 2.7 milyon müşterisinin banka bilgilerinin çalınması olaylarıyla görülmektedir. İlerleyen bölümlerde oluşabilecek siber tehditlerin boyutu ve etkileri risk analizi ile açıklanmaya çalışılmıştır.

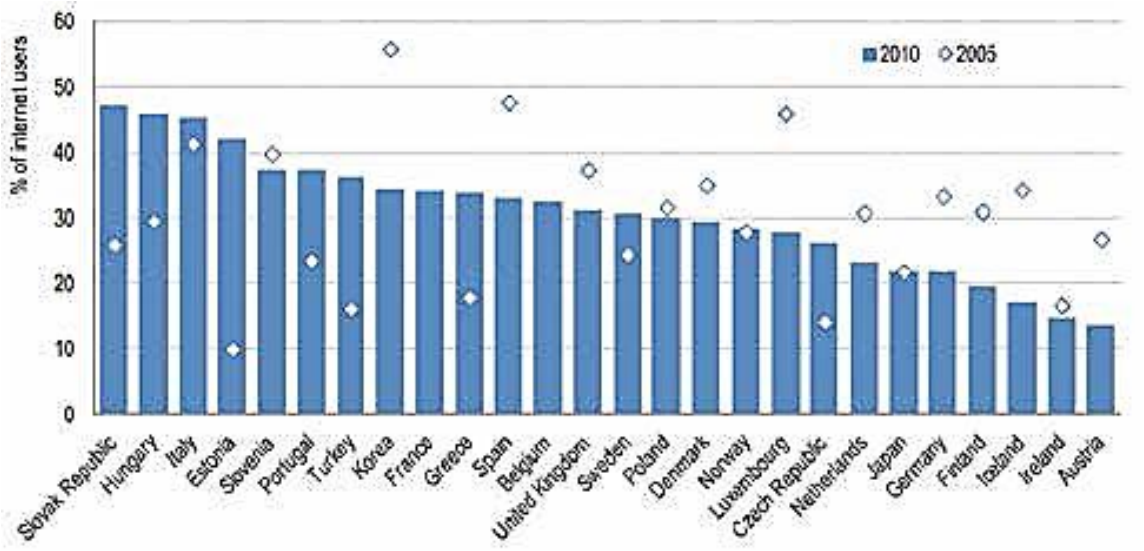
Güvenlik İhlali	Yüzde (%)
Yetkisiz (İzinsiz) Erişim	5.2
Hizmetlerin (Servislerin) Engellenmesi	0.1
Kötü niyetli program kodları	4.6
Uygunsuz Kullanım	8.3
Tarama / İzinsiz Giriş Denemesi	73.1
Araştırma İnceleme	8.7
Toplam	100.0

Kaynak: (US-CERT, 2007)

Şekil 2. E-Devlet Uygulamalarında Güvenlik İhlalleri
(Security Breach in E-Government Applications)

3. TÜRKİYE'NİN BİLGİ TOPLUMU STRATEJİSİ ve SİBER GÜVENLİK (TURKEY'S TRANSITION TO INFORMATION SOCIETY AND CYBER SECURITY)

Ülkemizde ve dünyada yaşanan tüm bu bilgi toplumuna geçiş süreci ile birlikte, bu sürece karşı olarak kişisel, ticari ve politik motivasyonlar barındıran zararlı yazılımların oranında büyük artış meydana gelmiş; ülkelerin kurum ve kuruluşları siber saldırıların hedefi olmuştur. Şekil.3'de yıllar içinde zararlı yazılımların artışı grafiksel olarak görülmektedir.



Şekil 3. OECD Verilerine Göre Bilgisayarına Virüs Bulaşan İnternet Kullanıcılarının Oranları [15]
(According To OECD Data; The Rate of Virus Infected Internet Users)

Bu konuda her geçen gün örnekler artmaktadır. Zararlı yazılımların sebep olduğu zararlar milyar dolarlar seviyesindedir. Zararlı yazılımlardan tarihten birkaç örnek verecek olursak;

- "I Love You" adlı virüsün dünya çapında yaklaşık 45 milyon bilgisayara bulaştığını ve yaklaşık 10 milyar USD'lik zarara,
- "Nimda" kurtçuğunun dünya çapında yaklaşık 3 milyar USD'lik, "Love Bug"ın ise 10 milyar USD'lik zarara,
- "MyDoom" adlı truva atının 4,8 milyar USD civarında zarara sebep olmuştur.
- "Sapphire/Slammer" solucanının 2003'te internete bağlı bilgisayarların % 90'ına 10 dakika içinde bulaşmıştır.
- 2005'in ilk altı ayında zarar gören bilgisayar sayısı bir önceki yıla göre % 63 artmıştır.
- ABD'li tüketicilerin son iki yılda bilgisayar tamiri ve yenilemesi için 7,8 milyar USD harcamıştır.
- 2008 yılında geliştirilen siber casusluk amaçlı kullanılan "Regin Virüsü" 2014 yılında fark edilmiş ve

Rusya, Sudi Arabistan, İrlanda, Belçika, İran gibi pek çok ülkeye yayılmıştır [5].

Özellikle bilgi toplumuna geçiş sürecini planlı ve sistemli yönetmeyen, tüm ülke için kritik olan altyapıların bilgi sistemlerinin yönetiminde ve denetiminde ulusal standart ve politikalar belirleyip kullanmayan ülkeler daha büyük risk altında olmuşlardır. Bunun en güzel örneğini 2007 yılında gerçekleşen Estonya-Rusya siber savaşında görebiliriz. Her ne kadar Estonya bilgi toplumuna geçiş sürecini başarılı bir şekilde yönetse de, bilgi varlıklarını korumak için siber güvenlik araçlarını uygulama konusunda aynı ölçüde titiz davranmamıştır. Bunun sonucunda trafik ışıklardan bankacılık işlemlerine tüm kamu ve özel bilgi sistemleri çökmüş NATO'dan yardım istemek zorunda kalmış ve ülke olarak büyük zarar görmüştür. Bu yüzden bilgi sistemlerine geçişten daha önemli olan, bunların güvenliğinin sağlanması ön plana çıkmaktadır [16].

Türkiye'de elbette uluslararası entegrasyon ve işbirliği ile ekonomik, sosyal, ticari ve kamusal faydalar sağlamak için bu geçişi süratle tamamlamaya çalışmaktadır. Fakat gerekli güvenlik altyapısını ve güvenlik politika ve standartlarını oluşturmadan uygulanan projeler; kritik altyapılarımızın güvenliği ve dolayısıyla ulusal güvenliğimiz açısından çok ciddi riskleri beraberinde getirebilecektir [3].

Günümüzde, küresel rekabette üstün olabilmek için birçok teori bulunmaktadır ama bunlardan en önemlisi insan kaynakları yönetimi ve eğitimidir. Fakat OECD verilerine göre Türkiye'nin GSMH' dan %1,9'luk eğitime ayırdığı pay ile bu konuda gerilerde olduğu görülmektedir. Yapılan bir araştırmaya göre "Araştırma ve Eğitim Hizmetlerine Erişim" göstergesinde Türkiye 2013-2014 döneminde 148 ülke içine 70. sırada bulunmaktadır. 2006 yılında 4.23 puan ile 44. sırada olan Türkiye 2013 yılında puanını aynen korumuş ancak diğer ülkelerdeki bu konudaki gelişmeler nedeniyle 70. sıraya gerilemiştir (Şekil.4). Yine de Türkiye bu göstergeye göre dünya ortalamasının(4.19) üzerindedir. Göstergede birinci sırada bulunan İsviçre'nin puanı 6,47'dir. Fikri mülkiyetin korunması ülkenin gelişmişlik seviyesi ile doğrudan ilişkili olan bir göstergedir. Ayrıca belki de eğitimin bir sonucu olarak değerlendirilebilecek, bu alanda ilk sıralarda bulunan ülkelerin tamamı yüksek kişi başına milli gelir düzeyine sahiptir [17].

Türkiye'nin Son 8 Yıllık Gelişimi

	2013-2014	2012-2013	2011-2012	2010-2011	2009-2010	2008-2009	2007-2008	2006-2007
Puan	4,23	4,04	4,09	4,24	3,88	3,88	4,34	4,23
Sıra	70	77	69	58	75	68	43	44

2013-2014 Döneminde En İyi On Ülke ve 8 Yıllık Gelişimleri

	2013-2014		2012-2013		2011-2012		2010-2011		2009-2010		2008-2009		2007-2008		2006-2007	
	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra
İsviçre	6,47	1	6,43	1	6,44	1	6,47	1	6,30	1	6,02	2	5,99	1	5,92	5
Almanya	6,10	2	6,09	4	5,98	3	6,21	2	6,03	2	5,81	5	5,98	3	6,07	3
Hollanda	6,09	3	6,13	2	6,00	2	6,02	4	5,97	4	5,83	3	5,81	7	5,70	8
Avusturya	6,09	4	6,09	3	5,96	5	5,89	6	5,55	12	5,23	16	5,32	15	5,32	14
Belçika	5,94	5	5,90	5	5,80	6	5,79	9	5,63	10	5,61	11	5,73	8	5,63	11
Finlandiya	5,87	6	5,67	8	5,64	10	5,81	7	5,94	5	5,82	4	5,71	9	5,82	6
Hong Kong	5,75	7	5,53	10	5,27	17	5,42	15	5,05	20	4,88	25	5,08	19	4,93	21
İsveç	5,69	8	5,77	7	5,97	4	6,11	3	5,84	7	5,73	7	5,89	4	5,59	13
ABD	5,67	9	5,60	9	5,63	11	5,76	10	5,98	3	6,12	1	5,99	2	6,14	1
Porto Riko	5,61	10	5,51	11	5,35	16	5,33	18	4,95	23	4,68	31	4,72	30		

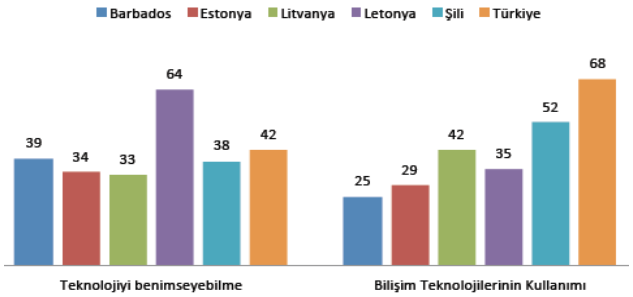
Şekil 4. Araştırma ve Eğitim Alanlarında Gelişmişlik Durumu
(Development Status In The Area of Research and Education)

Ayrıca diğer önemli hususta stratejiler belirlemek ve bu doğrultuda AR-GE çalışmaları yapmaktır. Bu sayede yeni teknolojilere mevcut sistemlerin adaptasyonu sağlanabilecek veya mevcut sistemleri geliştirmek için yeni teknolojiler ortaya çıkarılabilecektir. Bazı verileri incelediğimizde bilgi toplumuna geçiş sürecinin hangi aşamasında olduğumuz daha iyi anlaşılabilecektir [5].

Türkiye'nin içinde bulunduğu geçiş toplumu ülkeleri göz önüne alınarak 2013- 2014 yıllarında yapılan bir çalışmada "Teknolojik Altyapı" bileşeni incelendiğinde; Türkiye 2014 yılında 2013 yılına göre 5 basamak gerileyerek 58. sıraya düşmüştür [17].

Şekil.5 incelendiğinde ve diğer altyapılarla kıyaslandığında özellikle Türkiye'nin "Teknolojik

Altyapı" bileşeninde en çok "Bilişim Teknolojilerinin Kullanımı" alt bileşeninde 68. sıraya düştüğü görülmektedir. Yine aynı araştırmaya göre Türkiye'deki internet kullanıcı oranı endekste yüzde 45,13 olarak yer almaktadır. Türkiye bu oranla 148 ülke içinde 73. sırada yer almaktadır (Şekil.6). Türkiye bu oranla 148 ülke içinde 73. sırada bulunmaktadır.



Şekil 5. Teknolojik Altyapı Bileşenine Göre Türkiye'nin Sıralamadaki Yeri
(Turkey's Position In Technological Infrastructure Factor List)

Türkiye 2006 yılından bu yana göstergede puan açısından çok büyük bir gelişme göstermiştir ve puanı 3,49'dan 5,13'e yükselmiştir. Ancak diğer ülkeler daha büyük gelişimler gösterdiklerinden dolayı Türkiye'nin sıralaması 8 yıl içinde 55. sıradan 73. sıraya düşmüştür [17].

Türkiye'nin Son 8 Yıllık Gelişimi

	2013-2014	2012-2013	2011-2012	2010-2011	2009-2010	2008-2009	2007-2006	2006-2007
Puan	45,13	42,10	39,82	35,30	32,29	17,73	15,31	14,13
Sıra	73	69	64	65	54	68	62	55

2013-2014 Döneminde En İyi On Ülke ve 8 Yıllık Gelişimleri

	2013-2014		2012-2013		2011-2012		2010-2011		2009-2010		2008-2009		2007-2006		2006-2007	
	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra
İzlanda	96,00	1	95,02	1	95,00	1	93,46	1	67,20	17	65,30	11	87,76	1	77,00	1
Norveç	95,00	2	93,97	2	93,39	2	92,08	2	85,00	3	81,68	3	58,48	11	39,37	31
İsveç	94,00	3	91,00	4	90,00	5	90,80	3	80,00	5	76,97	5	76,21	2	75,46	2
Danimarka	93,00	4	90,00	6	88,72	6	86,84	6	84,90	4	58,23	16	52,55	15	50,36	17
Hollanda	93,00	4	92,30	3	90,72	3	89,63	4	86,76	1	85,71	2	73,99	3	61,63	10
Lüksemburg	92,00	6	90,89	5	90,62	4	87,31	5	78,00	8	72,01	7	67,74	8	59,00	11
Finlandiya	91,00	7	89,37	7	86,89	7	84,14	8	79,00	7	55,60	18	53,34	14	63,00	7
Yeni Zelanda	89,51	8	86,00	9	83,00	11	84,38	7	70,00	14	78,77	4	68,35	5	52,63	15
Katar	88,10	9	86,20	8	69,00	29	28,31	79	50,94	33	34,55	41	28,16	40	22,18	46
Bahreyn	88,00	10	77,00	21	55,00	41	82,04	11	33,22	49	28,44	47	21,33	48	21,30	47

Şekil 6. Ülkelerin İnternet Kullanıcı Oranları [17]
(Countries' Internet User Rate)

Türkiye'de Ar-Ge masraflarının Gayri Safi Yurtiçi Hasıla (GSYİH) içindeki payının TÜİK tarafından yapılan 2012 yılı Ar-Ge Faaliyetleri Araştırması sonuçlarına göre, ‰ 9.2 olduğu görülmüştür. Bu sürece uyumun önündeki en büyük engellerin güvenlik kaygısı ve erişim maliyetleri olduğu tespit edilmiştir. 2005 Bilgi Toplumu Stratejisi İşletmeler Araştırması'na göre Türkiye'de bilgi toplumuna geçişte en büyük engelin %46.1 ile güvenlik kaygısı olduğu, ikinci sırada erişim maliyeti olduğu tespit edilmiştir. 2012 yılına gelindiğinde oran değişse de sıralamanım değişmediği aynı araştırmada görülmektedir. Ayrıca, Ekonomik İşbirliği ve Kalkınma Teşkilatı'nın (OECD) yayınladığı bir rapora göre, üye ülkeler içinde saniyede mega bit ücreti açısından en ucuz geniş bant internet hizmetinin 0,22 dolarla Japonya; en pahalısının ise 81,13 dolarla Türkiye'de bulunduğu belirtilmiştir [3]. Türkiye geniş bant hizmeti açısından yapılan bir çalışmada 148 ülkeden 60. Sırada yer alarak dünya ortalamasının altındadır. Türkiye 2008 yılında Dünya ortalamasının üzerindeyken 2013 yılında dünya ortalamasının altına düşmüştür [17]. Aslında bunda en büyük sebep Türkiye'nin gerilemesi değil; yerinde sayması ve diğer ülkelerin gelişme göstermesidir. Bu uygulanan politika ve stratejilerin devamlılığının ve geliştirilmesinin zorunlu olduğunu bize göstermektedir.

Bilgi Toplumuna geçiş sürecinde önemli bir diğer unsurda yetişmiş personel ihtiyacıdır. Bu konuda Şekil.7 incelendiğinde her ne kadar 2011 yılında büyük ilerleme sağlansa da Türkiye'nin dünya ortalamasının altında olduğu ve bu konuyu ele alan politikaların gerekliliği ortaya çıkmaktadır. Tablonun böyle olmasındaki en büyük sebep atılan adımların geliştirilmemesidir veya mevcut duruma göre yeni stratejiler belirlenmemesidir. Örneğin 2012 yılında stratejik eylem planında siber güvenlik alanında üniversitelerde yüksek lisans ve doktora programlarının açılması kararına rağmen bu birkaç üniversiteyle sınırlı kalmıştır.

Renk Skalası			6	5	4	3	2	1
			Düşük Sıralama					Yüksek Sıralama
No	Gösterge	Açıklama	2008	2009	2010	2011	2012	2013
			134 Ülke	133 Ülke	139 Ülke	142 Ülke	144 Ülke	148 Ülke
12.06	**Bilim İnsanı ve Mühendis Erişilebilirliği**	İnovasyon kapasitesinin, doğrudan insan kapasitesi ile ilişkilidir. Bu çerçevede ülkenin her yerinde bilim insanı ve mühendis mevcudiyeti önem taşımaktadır. Endekste bilim insanı ve mühendislere, ulusal düzeyde erişim olanağı değerlendirilmektedir.	59	51	44	35	41	53

Şekil 7. Türkiye'nin Yetişmiş İnsan Durumu [17]
(Turkey's Educated Person Condition)

Türkiye'nin mevcut bilgi toplumu durumunu yukarıda verdiğimiz istatistiksel bilgiler ışığında değerlendirmeyi müteakip siber güvenlik stratejisine bakmakta fayda vardır. Bu alanda çalışmalar bilgi toplumuna geçiş sürecinin gerisinde kalmıştır. Bu konuda özellikle teknik altyapı ile hukuksal düzenlemeler eş zamanlı yürütülememiştir. Bunda en büyük sebep bilgi toplumuna geç geçiş süreci ve bilgi üretim toplumu olamayışımız nedeniyle bilgiye zor ve pahalıya ulaşmamız ve planlanan stratejilerin altyapı yetersizliği ve farkındalık eksikliği nedeniyle hayata geçirebilmede yaşanan sıkıntılar olduğu söylenebilir. Bu yüzden yapılan hukuksal düzenlemeleri hayata geçirmek zaman almış siber tehditler şekil değiştirmeye devam etmiş, çağın gerisinde kalınmıştır. Bu konudaki bazı düzenlemeler;

- 2004- 5070 sayılı Elektronik İmza Kanunu,
- 2008- Elektronik Haberleşme Güvenliği Yönetmeliği,
- 2006- 2006/38 sayılı Yüksek Planlama Kurulu Kararında bulunan Bilgi Toplumu Stratejisi ve Eki Eylem Planı,
- Siber güvenliğe ilişkin olarak makro planda atılmış en somut adım 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" dır.

Atılan bu adımlar gün geçtikçe bilgi toplumuna geçiş hızlandıkça siber bağımlılığımızı artırmaktadır ve buna bağlı olarak da siber risklerin boyutu büyümektedir. Siber Güvenliğin sağlanması için aşağıdaki sıra çerçevesinde sistemli bir şekilde çalışmaların yürütülmesi gerekmektedir [5].

1. Ulusal politika ve stratejinin geliştirilmesi
2. Yasal çerçevenin oluşturulması
3. Teknik tedbirlerin geliştirilmesi
4. Kurumsal yapılanmanın belirlenmesi
5. Ulusal işbirliği ve koordinasyonun sağlanması
6. Kapasitenin geliştirilmesi
7. Farkındalığın artırılması
8. Uluslararası işbirliği ve uyumun sağlanmasıdır.

Siber stratejilerin uygulanması için öncellikle bu maddeleri uygulamaya sokacak merkezi kurumların oluşturulması ve bunların koordineli çalışması gerekmektedir. Ayrıca bunların denetimlerinin sürekli yapılabilmesi için iç denetim mekanizmaları oluşturulması zorunludur. Çünkü siber dünya sürekli olarak şekil değiştirmekte, alınan önlemler tehditler için çoğu zaman yeterli olmamaktadır [15].

Toplumumuzun giderek internete bağımlı hale geldiği, aynı zamanda bilgi teknolojileri saldırılarına karşı açıklıkların arttığı, bunun en büyük nedeni olarak da, teknoloji ve küreselleşmede yaşanan büyük hız, kanunlar ve yasal prosedürlerin ve politikaların mücadele edememesi gösterilmektedir [15]. Bununla birlikte erişim maliyetleri, yetişmiş personel yetersizliği ve teknik tedbirlerin geliştirilememesi yaşanan olaylar dikkate alındığında üzerinde durulması gereken konular olarak

karşımıza çıkmaktadır. Çünkü her ne kadar ülkemizde politikalar ve hukuksal düzenlemeler yapılmasında bir ivmelenme göze çarpsa da bunları uygulamada karşımıza çıkan teknik altyapı yetersizlikleri bu kuralları somut adımlara dönüştürememektedir. Küreselleşmenin yarattığı rekabet zorunluluğu ülkeleri bilgi teknolojileri gibi dinamik bir alanda sürekli yeni politikalar ve stratejiler üretmeye zorlamaktadır. Geçmiş yıllar incelendiğinde Türkiye'nin olumlu olarak geçte olarak bu alanda somut adımlar attığı ama özellikle 2008 yılından sonra bu adımları devam ettiremediği ve yeni adımlar atamadığı çalışmamızdaki istatistiklerde görülmektedir. Bu yüzden diğer ülkelerin ilerleyişi karşısında dünya ortalamasının altına düşmüştür ve siber ortamda mücadele gücü zayıflamıştır.

4. KRİTİK ALTYAPILAR VE SİBER TEHDİT UNSURLARI (CRITICAL INFRASTRUCTURE AND COMPONENT OF CYBER THREATS)

Dünyanın büyük bir hızla gelişmesi, küreselleşmesi ve sanayileşmenin etkisiyle birlikte, coğrafi olarak dağınık ve büyük bir alana yayılan altyapı tesislerinin yönetimi için uzaktan kontrol ve erişim sistemleri kullanılmaya başlanmıştır. Bu sayede uluslararası çalışmalarda ülkelerin işbirliği ve bütünleşme çalışmaları bilgisayar sistemleri sayesinde kolaylaşmış ve hızlanmıştır. Buna örnek olarak Türkiye'nin elektrik kritik altyapısını 2010 yılında Avrupa'ya entegre ettiği ENTSO-E (Avrupa Kıtası Senkron Bölgesi Şebekesi)'yi örnek verebiliriz. ENTSO-E çatısı altında; 34 Avrupa ülkesinden 41 İletim Sistemi İşletmecisi Denetleme Kontrolü ve Veri Elde Etme (Supervisory Control and Data Acquisition-SCADA) sistemleri aracılığıyla birbirine bağlanmıştır. Böylece ülkelerin tüm altyapılarını kontrol eden bilgi sistemlerinin korunma ihtiyacı ortaya çıkmıştır. Özellikle bazı altyapıların zarar görmesi milli güvenlik ve sosyal hayat açıdan daha büyük etki yaratmasıyla "kritik altyapı" ayrımına gidilmiştir [18].

Kritik altyapılar kamu huzuru için hayati önemi olan fiziksel ve mantıksal kolaylık tesisleridir. Bu altyapılar; elektrik üretim ve dağıtım, yollar, köprüler ve tüneller gibi ulaşım sistemleri, havayolu ve hava trafik kontrol sistemleri, iletişim ağları, su depolama ve dağıtım sistemleri, yiyecek depoları, tıbbı ve sağlık sistemleri, finansal, bankacılık ve ticaret sistemleri olarak sınıflandırılabilir. Bu sistemler deprem, kasırga gibi doğal afetlerin, savaşların, ayaklanmalar gibi sosyal krizlerin ya da terörist aktivitelerin hedefi olabilir. Ancak son yıllarda kritik altyapılara geçekleştirilen ve medyaya da yansıyan saldırılar dikkate alındığında, bu saldırıların büyük çoğunluğu haberleşme altyapısına ya da haberleşme altyapısı aracılığıyla yapıldığı görülmektedir [19]. Türkiye'de kullanılan bilgi ve haberleşme altyapısı incelendiğinde dış kaynaklardan temin edilen güvenlik sistemlerinin olduğu fark edilmektedir. Bu da siber bağımlılığı ve açıklıkları beraberinde getirmektedir [20].

Bilgi ve teknoloji altyapılarındaki gelişmeler kritik altyapılarının yönetiminde önemli değişiklikler meydana getirdiği, bunun sonucunda da daha önceleri tanımlanmayan, yeni açıklıkların ortaya çıktığı önceki bölümde açıklanmıştır. Tüm dünyada ülkeler bu yeni teknolojilere, ortaya çıkarabileceğe açıklıklara ve mevcut ülke potansiyellerine aldırmadan ayak uydurmaya çalışmaktadırlar. Oysa her ülkenin teknolojik kapasitesi, yeteneği ve hazır olma potansiyelleri Tablo 3'de görüldüğü gibi farklı olabilmektedir. Bazı ülkeler hızlı sürece ayak uydurabilecekken bazıları bu durumdan büyük zararlar görebilmektedir.

Tablo 3. Ülkelerin Bilgi Toplumuna Hazır Olma Durumları [3]
(The State of Countries' Availableness To Information Nation)

SIRA	ÜLKE	PUAN
1	Singapur	1.73
2	İzlanda	1.66
3	Finlandiya	1.62
4	Damirka	1.60
5	ABD	1.58
6	İsveç	1.53
7	Hong-Kong	1.39
8	Japonya	1.35
9	İsviçre	1.30
10	Kanada	1.27
...	.....	.....
52	**TÜRKİYE**	**-0.14**
TOPLAM 104 ÜLKE		

Örneğin Siber bağımlılığın oldukça fazla olduğu ABD'de bu yaşanan değişimi şu şekilde gerçekleşmiştir. 1997 yılında başkanın kritik altyapıların güvenliği konusunda yaptığı açıklamalarda, ABD'nin kritik altyapılarının yeni açıklıklara-siber açıklıklara ve yeni tehditlere-siber tehditlere maruz kalacağı, geçmişte ABD'ye iyi hizmet ettiğini düşünülen savunma sisteminin siber tehditlere karşı fazla koruma sağlamayacağı belirtilmiştir. Kritik altyapı olarak değerlendirilen; enerji, bankacılık, finans, ulaşım ve kritik servisler ve telekomünikasyonun bilgi çağı kapsamında tekrar değerlendirilerek, altyapıların bağımsız bir bilgisayar ve haberleşme ağı ile birbirine bağlı olması gerektiği değerlendirmesi yapılmıştır [21]. Ancak toplumun ihtiyaçları ve refahı için, bilgi teknolojilerinin özellikle de internet ağı kritik altyapılarda

kullanılmaya başlanmış, ABD ise en yaygın olarak kullanan ülkelerden biri haline gelmiştir. Özellikle 11 Eylül saldırıları ABD'nin siber bağımlılığını ve bilgi güvenliği için gerekli önlemlerin alınmadan, kamuya ait bilgilerde dahil olmak üzere açık kaynak olarak yayımlamaktaydı. Ancak ABD, özellikle 2001 yılında yaşanan 11 Eylül saldırılarından sonra, ulusal güvenlik politikalarını, sivil haklar, özgürlükler ve sınır kavramını değiştirmiştir. Özellikle, ifade özgürlüğü, bilgiye erişim ve gizlilik politikalarında önemli değişiklikler yapmıştır. Kamu alanında bilgi; artık serbest, açık ve demokratik ulusa zarar verme potansiyeli olan bir silah olarak tanımlanmıştır. Bu nedenle, açıklık ve şeffaflıktan gizlilik ve özellikle kamuya ait bilgilere erişimde sınırlamalara doğru bir değişim süreci yaşanmıştır. Örneğin Çevresel Koruma Kurumu (The Environmental Protection Agency) kimyasal fabrikaların ve depolama merkezlerinin yeri ile olası bir tehlike anında sağlığı etkilenebilecek insanların haritasını internet ortamından kaldırmıştır [22].

Kritik altyapılarda kullanılan bilgi sistemlerinin korunması için risk analizi için yapılması ve bu doğrultuda sistemi oluşturan varlıklar belirlenmesi, daha sonra ise bu varlıkların birbiri ile olan bağlantısını, erişilebilirlik durumlarını gösteren oluşturulması ve varlıkların kurum/kuruluş yönünden kritikliklerine ve önem derecelerine göre taktik, operatif ve stratejik seviyelere ayırarak bölümlendirilmesidir. Erişilebilirlik matrisi ve seviye bölümlendirmesinin oluşturulması durumunda, risk değerlendirme sürecinin tamamlanmasını müteakip risk azaltma sürecinde ilk müdahale edilecek varlıklar, hatanın tespit edildiği varlığa erişen (bağlantısı olan) diğer varlıklar tespit edilerek, diğer varlıkları analiz kapsamı dışında bırakılabilecektir. Bu sayede tepki süresi kısalacak ve sistemlerin alacağı hasar en aza indirilebilecektir [23]. Yapılan bu test ve analizler sonucunda kritik kabul edilen altyapılarda durumsal farkındalık oluşturulabilecektir.

Kritik altyapıların siber güvenliğinin sağlanması için ihtiyaç duyulan konulardan birisi de, kritik altyapının yönetiminden sorumlu kamu kurum kuruluşları ile özel sektör kurum ve kuruluşları arasında güvenli veri iletim ağlarının oluşturulmasıdır. Özellikle birbirine bağımlı altyapılar dikkate alındığında, bir altyapıda meydana gelen bir saldırı ya da hata diğer altyapıları da etkileyeceğinden, güvenli ağ üzerinden uyarı/ikaz sistemi geliştirilmesi altyapıların erken müdahale ve önlem almasını sağlayabilecektir. Avrupa Birliğinin Kritik Altyapı Uyarı Bilgi Ağı (Critical Infrastructure Warning Information Network-CIWIN) ABD'de ise İç Güvenlik Departmanı (Department of Homeland Security-DHS) tarafından geliştirilen CWIN, Avutralya'nın Kritik Altyapıların Korunması için Güvenilir Bilgi Paylaşım Ağı (Trusted Information Sharing Networks for Critical Infrastructure Protection-TISNCIP) bu ağlara örnek olarak verilebilir [24].

Yukarıda belirtilen siber tehdit unsurlarına rağmen uluslararası ilişkilerde, rekabette söz sahibi olabilmek ve bütünleşme sayesinde ekonomik faydalar kazanmak, iş hayatında ve sosyal hayatta yöneticiler, çalışanlar ve kurumlara getirdiği avantajlar ve kolaylıklar sayesinde bilgi teknolojilerini kullanmak artık zorunlu hale gelmiştir. Türkiye'de bu bilgi ve iletişim ortamına geçiş yapabilmek için 20. Yüzyılın sonlarına doğru çeşitli çalışmalar ve projeler yürütmeye başlamıştır.

5. ANALİZLER VE ÇIKARIMLAR (ANALYSIS AND INFERENCES)

Bilgi teknolojilerinin özellikle de internetin, hayatımızın her alanına girdiği günümüzde, söz konusu teknolojiler toplumlara ve kurumlara her açıdan fayda getirmiş ve sağladığı hizmetlerle ciddi anlamda kolaylıklar sağlamıştır. Fakat kullanılan teknoloji ve uygulamalar; toplumları, kurumları ve devletleri bu altyapılara bağımlı hale getirmiştir. Bilgi teknolojileri, zarar görmesi, saldırıya uğraması veya çalışmasında yaşanan aksaklıklardan dolayı hizmet verememesi durumunda çok ciddi sonuçlar doğurabilecek risklerle karşı karşıya bırakabilecek, toplum düzenini bozabilecek hatta ulusal güvenliği tehlikeye atabilecek altyapılar haline gelmiştir. Çünkü bilgi teknolojilerinin bu kadar yoğun kullanılması sonucu bireyler olarak siber bağımlı bireyler, daha genel anlamda da toplum ve ulus olarak da siber bağımlı toplum ve siber bağımlı ulus olma yönünde çok hızlı adımlar ve gelişmeler yaşanmaktadır. Bunların başında, önceki bölümde açıklanan bilgi toplumuna geçiş süreci bulunmaktadır. Bu geçiş süreci daha çok verilerimizi, bilgilerimizi sayısal ortama aktarma aşamasında başarılı olmuş ancak bunun paralelinde bu bilgilerin güvenliğini sağlayacak düzenlemeler konusunda aynı başarı gösterilememiştir. Bu kapsamda, bilgi teknolojilerinin beraberinde getirdiği tehdit ve risklerden sakınmak için tamamlanması gereken eksikler ve açıklıklar bulunmaktadır.

Bu eksikliklerden ilki, özellikle bilgi güvenliği ile ilgili bölümde çalışacaklar başta olmak üzere, tüm personelimizin bilgi güvenliği konusunda yeterli eğitimi almamalarıdır. Eğitimin de yaşayan, canlı bir süreç olması gerektiği dikkate alınarak, bilim ve teknolojideki

gelişmelere (ortaya çıkan yeni tehditler, yeni saldırı yöntemleri ve alınması gereken tedbirler) paralel olarak kurum içinde tazeleme eğitimleri planlanmalıdır.

Ele alınması gereken ikinci konu, toplumun bilgi güvenliği ve önemi konusunda farkındalığının artırılması ve bilinçlendirilmesidir. Bu kapsamda, ilköğretim okullarından itibaren başlamak üzere eğitim müfredatına bilgi güvenliği konusunun dâhil edilmesi gerekmektedir. Bilgisayar kullanım yaşı dikkate alındığında bunun önemi ortaya çıkmaktadır. Özellikle üst düzey yöneticiler ve bilgi güvenliği alanında çalışan personel başta olmak üzere, tüm bireylere (bilgi teknolojilerini kullanan tüm personele) farkındalığın oluşması ve bu konuda bilgilendirmek amacıyla eğitim planlanmalıdır.

Dikkat edilmesi gereken üçüncü husus yetkilendirmedir. Kurum ve kuruluşlar içinde bilmesi gereken prensibi ile yetkilendirme yapılmalı, oluşturulan kullanıcı adı ve etkili şifreleme sistemleri vasıtasıyla tüm çalışanların her bilgiye erişmesine müsaade edilmemelidir. Ayrıca kurum ve kuruluşlarda açık anahtar altyapısı kurarak, evrakların yetkisiz kişiler tarafından erişilmesi, değiştirilmesi ve kopyalanması engellenmelidir. Özellikle bilgi güvenliği açısından kritik olan yazılımlar konusunda çalışan personelde görev ayrımının yapılmasına özen gösterilmelidir. Yazılımları gerçekleştiren birimler ile test yapan birimler aynı kişilerden oluşmamalıdır. Bu sayede yazılımlar içine yerleştirilebilecek açık kapıların, hataların, zafiyetlerin (açıklıkların) tespit edilmesi kolaylaşacaktır.

Diğer bir husus da, kritik personelin yedekli çalıştırılmasıdır. Bu sayede, söz konusu personelin kontrolü yapılacak, hem de kritik personellerin herhangi bir sebeple görevden ayrılmaları gerektiğinde sistem sekteye uğramadan faaliyetini devam ettirebilecektir [25]. Unutulmamalıdır ki, bir sistem için en tehlikeli bileşen (varlık), üst seviyede erişim ve değiştirme yetkisi olan personeldir. Çünkü söz konusu personelin herhangi bir nedenle yetkisini kötüye kullanması durumunda sistemleri geri dönüşü imkânsız olabilecek sonuçlarla karşı karşıya bırakabilir.

Siber bağımlılığın önemli ölçüde arttığı günümüzde oluşan beşinci eksiklik, milli bilgi sistem yazılım ve donanım ürünlerinin üretilmesidir. Siber dünyada yaşanan bilgi güvenliği ihlalleri göz önüne alındığında milli olmayan ürünlerde güvenlik açıklıkları daha fazla oluşabilecektir. Güvenlik boyutunun bir bileşeni de, yazılım ve donanım güvenliğidir. Bunu sağlamak için milli ürünler geliştirilmelidir. Bu konuda da üniversite sanayi işbirliğinin yapılabilmesi süreci hızlandıracaktır.

Göze çarpan altıncı eksiklik tüm kurum ve kuruluşların kendilerine has sürekli ve yenilenen dinamik bir risk analizi yapmamalarıdır. Toplum düzeni ve ulusal güvenlik açısından büyük önem taşıyan kritik altyapıların risk analizi sürecinde değerlendirilmesi hayati öneme sahiptir. Dünyada birçok gelişmiş ülkede; elektrik, su, doğal gaz, enerji gibi birçok kritik altyapı uzaktan erişimle kontrol edilmektedir. Ancak, uzaktan erişim ve sayısallaşma, kazandırdığı avantajların yanında riskleri de beraberinde getirmektedir. Modern kritik altyapılar, yaygın olarak bilgi ve haberleşme teknolojilerini kullanmaları nedeniyle oluşan mimari zayıflık ve açıklıklar nedeniyle sürekli olarak yeni tehditlere maruz kalmaktadırlar.

Risklerin mevcut olması teknolojik imkânlardan kaçınılmasını değil, yeni teknolojilerin beraberinde getirdiği tehditlerden sakınmayı gerektirmektedir. Bunun da yolu, açıklıkları mümkün olduğu kadar en aza indirmek maksadıyla, kritik altyapılarımız başta olmak üzere, kamu kurum/kuruluşlarımız ile önem arz eden özel sektör kuruluşlarımızın bilgi sistem ve iletişim altyapılarının sürekli olarak izlenmesi, kontrol altında tutulması ve güvenlik açıklıklarının tespitine yönelik gerekli analizlerin yapılması gerekmektedir. İşleyen sistem üzerinde güvenlik analizleri ve testler yapmak hem işlerin aksamasına hem de testler esnasında meydana gelebilecek hatalardan dolayı sistemin zarar görmesine neden olabilir. Bundan dolayı, sistemin tüm varlıklarının (ya da en azından kritik olarak değerlendirilenlerin) bir sınama ortamı (testbed) üzerinde farklı yöntemlerle benzetiminin yapılarak risk analizlerinin yapılması oldukça önemlidir. Bu sayede, sistemimizin açıklıkları (güncel saldırı teknikleri de dâhil edilerek) güncel olarak tespit edilebilecek ve gerekli önlemler alınabilecektir [26].

Uzaktan erişim yapılan her sistemde olduğu gibi kritik altyapıları yöneten sistemlerde de (SCADA gibi), gerekli güvenlik önlemleri alındığı takdirde sistem deki açıklıklar en aza indirilebilecektir. Bu önlemlerden ilki, yazılım ve donanımlardır. Uzaktan erişim için kullanılan VPN, DMZ ve firewall yazılım ve donanımları sürekli güncel halde tutulmalı ve dışarıdan gelebilecek saldırılara karşı uyarı (IDS, IPS) sistemleri eklenmelidir. İkinci olarak, uzaktan erişim yapan kullanıcılar için çoklu şifreleme/güvenlik sisteminin oluşturulmasıdır. Toplum için hayati öneme sahip olduğunu ifade ettiğimiz ve dış tehditlerin ilk hedefleri arasında bulunan kritik altyapılara erişimin basit şifreleme teknolojisiyle yapılması ya da varsayılan (default) şifrelerin kullanılması önemli riskleri ortaya çıkaracaktır. Bu nedenle, akıllı kart, biyometrik okuyucu,

sms ile şifre gönderimi, katmanlı şifre yapısı gibi uzaktan erişimi zorlaştırıcı tedbirler alınması gerekmektedir.

Neredeyse tüm altyapılarımızın siber ortama bağlı hatta bağımlı olduğu günümüzde, kurum ve kuruluşlarımız için kritik olarak kabul edilen bilgilerimizi yedeklemek maksadıyla, mümkün olduğu kadar çıktı alarak dosyalamalı (hard copy) ve bu bilgilerin bulunduğu bilişim sistemlerinin dış ağlardan bağımsız olması sağlanmalıdır.

Siber ortama geçiş sürecinde diğer bir husus; hukuki yapılanma için atılan adımlardır. Bunlardan ilki, bilgi güvenliğinin sağlanmasına yönelik olarak "Bilişim Alanında Suçlar" başlığı altında yapılan kanunlarımızdır. "Bilişim sistemine yetkisiz erişim ve kalma" (TCK Md. 243) ile başlayan, "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" (TCK Md. 244) kanun maddesiyle devam eden kanunlarımız incelendiğinde, cezaların oldukça düşük, caydırıcılıktan öte suça teşvik eden bir yapısı bulunduğu görülmektedir.

Hukuki alanda yapılan düzenlemelerden; Kayıtlı Elektronik Posta (KEP) Kullanımı ve Elektronik İmza düzenlemelerini örnek olarak değerlendirildiğinde, KEP uygulaması ile alıcı ve gönderici kullandıkları elektronik imza sayesinde, mesajın bütünlüğü, doğru adrese gönderildiği, teslim edildiği garanti altına alınmaktadır. Bu gibi uygulamaların yaygınlaşması ve kullanılması ise, kurumların (özellikle de üst kademe yöneticilerin) bilgi güvenliği alanındaki farkındalıklarının gelişmesiyle ve özdenetim de dâhil olmak üzere etkin denetleme mekanizmasının oluşturulmasıyla gerçekleşebilir. Kanun ve düzenlemelerin hazırlanması için geçen süre, bunların denetlenmesi ve takibi ile geçen süreye kıyasla oldukça kısadır. Süreç olarak kanun ve düzenlemeleri hazırlamada gösterdiğimiz başarıyı denetleme ve takip konusunda gösteremediğimiz sürece bu alanda da başarılı olamayız. Bu nedenle, gerekli yasal düzenlemeleri oluşturmayı müteakip, öz denetim başta olmak üzere ihtiyaç duyulan denetleme ve kontrol mekanizmalarının da oluşturulması gerekmektedir.

Ülke olarak her ne kadar pek çok alanda siber bağımlılık düzeyimiz yüksek olsa da yukarıda belirtilen hususlar siber savunma gücümüze olumlu etki edecektir. Bu sayede bu geçiş sürecinin en az zararla atlatılması sağlanabilecektir. Ülkelerin siber bağımlılığı, sahip oldukları siber savaş ve siber savunma gücünü de yakından etkilemektedir. Ülkelerin siber savaş kapasitesinin belirlenmesinde, siber savaş kabiliyeti açısından olumlu bir katkıda bulunan bir unsur (bilgi ve iletişim ağı altyapısının yaygınlığı gibi) aynı zamanda siber saldırılara karşı hedef de olduğundan, siber bağımlılık ve siber savunma açısından da negatif olarak da etkileyebilen bir ikilem olarak karşımıza çıkabilmektedir [27].

ABD Ulusal Güvenlik Koordinatörü, Kritik Altyapıları Koruma ve Anti-Terör Başkanı olan Richard Clarke' a göre, siber savaş gücü demek sadece saldırı kabiliyeti demek değildir. Bu konuyu "siber sistemlere olan bağımlılık" ve "siber savunma" faktörleri de etkilemektedir. Buna göre bazı ülkelerin siber savaş kabiliyetleri basitçe Tablo 4'te görülmektedir [28].

Tablo 4 incelendiğinde, "Siber Saldırı" ve "Siber Savunma" bileşenlerinin "Siber Savaş" ile doğru orantılı, "siber bağımlılık bileşeninin ters orantılı olduğu görülmektedir. Bu nedenle, verilen puanlarda, siber saldırı ve savunma kabiliyeti yüksek olan ülkeler en yüksek puanı almış, siber bağımlılık konusunda ise; siber bağımlılığı yüksek olan ülkeler daha düşük puan, bağımlılığı düşük olan ülkeler ise, daha yüksek puan almıştır.

Tablo 4. Ülkelerin Siber Savaş Kabiliyetleri
(Capabilities of Countries' Cyber War)

Ülke	Siber Saldırı	Siber Bağımlılık	Siber Savunma	Toplam
ABD	8	2	1	11
Rusya	7	5	4	16
Çin	5	4	6	15
İran	4	5	3	12
Kuzey Kore	2	9	7	18

6. TARTIŞMA VE SONUÇLAR (DISCUSSION AND CONCLUSION)

Siber güvenlik konusunda gelişmeler ve teknolojiler o kadar hızlı ilerlemektedir ki ülkemizde yapılan düzenlemeler suçlarla ve saldırılarla mücadelede yetersiz kalmaktadır. Küresel olan bu tehditlere karşı koymak için ulusal düzenlemeler ve milli çözümler gerekmektedir. Ayrıca kamu ve özel sektör maliyet ve gizli bilgi endişelerine rağmen koordineli çalışması gerekmektedir. Getirdiği denetim kolaylığı ve uluslararası entegrasyon sağlama avantajlardan ötürü kritik altyapılarda bilgi sistemlerinin kullanılması güvenlik konusunda gerekli milli önlemler alınmadığı sürece getirebileceği riskler büyük olacaktır.

Türkiye'de siber güvenlik henüz tam anlamıyla anlaşılamamış, önlem alınamamış ve yeterli olgunluğa erişememiş bir kavramdır. Bu alanda mevcut güvenlik güçlerinin imkân ve kabiliyetleri ile yetişmiş personel sayısı çok düşük sayıdadır. İnternet ortamında işlenen suçlara müdahalede uluslararası roller de eklenince bu sayı yetersiz kalmaktadır. Son dönem siber saldırıların sayılarında büyük bir artış meydana gelmesiyle bu konuda olumlu ve ümit verici çalışmalara hız verilmiştir. Bunlara örnek olarak Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Programı, Ulusal Bilgi Güvenliği Kapısı, Yasal Çalışmalar, Siber Olaylara Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, Konferanslar, Çalıştaylar ve de TSK bünyesinde icra edilen faaliyetler ve oluşumlar verilebilir.

Ulusal ve uluslararası faydalar nedeniyle bilgi toplumuna geçiş kaçınılmazdır. Fakat bu sürecin güvenlikle birlikte yönetilmesi ve hizmetlerin aksamadan yürütülmesi gerekir. Aksi takdirde ülke olarak telafisi olmayan olaylarla karşılaşabiliriz. Bu nedenle; bilgi güvenliği alanında titiz bir planlama, kontrol, özel sektör ve kamuya ait ulusal kurumları arasında koordinasyonun sağlanması, uluslararası platformlarda işbirliği ve uyum, farkındalık, eğitim ile milli çözümler ciddi problemler ile karşılaşmadan dikkate alınması gereken konulardır. Bilginin en değerli varlık ve bilgiye sahip olanın güce sahip olduğu bir ortamda, bilginin elde edilmesi kadar, korunmasının da hayati öneme sahip olduğu, bunun için de yukarıda belirtilen önlemlerin alınması gerektiği değerlendirilmektedir.

KAYNAKLAR (REFERENCES)

[1] M. N., Öğün ve A. Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri,*18, 145-181, 2009.

[2] İnternet: AV-Test Şirketinin Yaptığı Araştırma, http://www.threattracksecurity.com/it-blog/year-end-malware-stats-from-av-test/, 03.03.2015.

[3] M. A. Çukurçayır, E. Çelebi, "Bilgi Toplumu ve E-Devletleşme Sürecinde Türkiye", *ZKÜ Sosyal Bilimler Dergisi*, 5(9), 59–82, 2009.

[4] H. Ö. Sancak, S. Güleç, "Küreselleşme-Bilgi Teknolojileri-Değişim: Türkiye'de Kamu Örgütlerinde Örgüt Yapısı Açısından Bir İnceleme", **VII. Kamu Yönetimi Forumu,** Sütçü İmam Üniversitesi, Kahramanmaraş, 154-169, 8-10 Ekim, 2009.

[5] İnternet: M. Ünver, C. Canbay, Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik, Bilgi Teknolojileri Kurumu, http://www.btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/dokumanlar/siber_guvenlik.pdf, 10.05.2015.

[6] Y. Yılmaz, "Transition to Knowledge Society in Turkey: Current State and Future Perspectives", Marmara University, Taylor&Francis Group, *Turkish Studies*, 13(3), 509–522, 2012.

[7] J. B. Burnham, "Telecommunications policy in Turkey: Dismantling Barriers to Growth", *Telecommunications Policy*, 31, 197–208, 2007.

[8] G. Maraş, "Kamu Yönetimlerinde E-Devlet Ve E-Demokrasi İlişkisi", *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 37, 121-144, 2011.

[9] Y. Demirhan, İ. Türkoğlu, "Türkiye'de E-Devlet Uygulamalarının Bazı Yönetim Süreçlerine Etkisinin Örnek Projeler Bağlamında Değerlendirilmesi", *Uluslararası Yönetim İktisat ve İşletme Dergisi*, 10(22), 235-256, 2014.

[10] A. Efendioğlu, E. Sezgin, "E-Devlet Uygulamalarında Bilgi ve Paylaşım Güvenliği" *Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi,* 16(2), 219-236, 2007.

[11] W. M. Fadhıl, A. Sökmen, E. B. Ekmekçioğlu, "Geleneksel Devlet Anlayışından E-Devlete: Türkiye ve Irak E-Devlet Algısı Karşılaştırması", *Bilişim Teknolojileri Dergisi*, 7(3), 21-29, 2014.

[12] F. K. Çelen, A. Çelik, S. S. Seferoğlu, "Türkiye'deki e-Devlet Uygulamalarının Değerlendirilmesi", **Akademik Bilişim**, İnönü Üniversitesi, Malatya, 1-9, 2-4 Şubat 2011.

[13] İ. Sevinç, "Türkiye Kamu Yönetiminde Bilgi Teknoljileri Kullanımı", Selçuk Üniversitesi İktisadi ve İdari Bilimler Fakültesi, *SB Meslek Yüksek Okulu Dergisi*, 355-371, 2005.

[14] E. Kumaş, B. Birgören, "E-Devlet Kapısı Projesi Bilgi Güvenliği ve Risk Yönetimi: Türkiye Uygulaması", *Bilişim Teknolojileri Dergisi,* 3(2), 29-36, 2010

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

[16] A. Ağır, "Bilişim Toplumuna Geçiş Sürecinde Bilgi Yönetimi Yaklaşımı", *İletişim Fakültesi Dergisi*, 5-17, 2007.

[17] F. Ulengin, Ş. Ö. Ekici, E. Tamer, **Türkiye'nin Küresel Rekabet Düzeyi Küresel Endekslerde Türkiye'nin Rekabet Gücüne İlişkin Bir Değerlendirme,** TÜSİAD Sabancı Üniversitesi Rekabet Forumu, İstanbul, 2014.

[18] S. Rautmare, "SCADA System Security Challenges and Recommendations", **India Conference (INDICON), Annual IEEE,** 1-5, 16-18 Aralık 2011.

[19] S. K. Das, K. Kant, N. Zhang, **Handbook on Securing Cyber-Physical Critical Infrastructure**, Elsevier, 2012.

[20] A. El Kalam, ve diğerleri, "PolyOrBAC: A Security Framework for Critical Infrastructures", *International Journal of Critical Infrastructure Protection*, 154-169, 2009.

[21] Critical Foundations Protecting America's Infrastructıres, **The Report of President's Comission on Critical Infrastructure Protection**, USA,1997.

[22] N. Caidi, R. Anthony., "Information Rights and National Security", *Government Information Quarterly*, 22(4), 663-684, 2005.

[23] G. Jian ve diğerleri. "A Digraph Model for Risk Identification and Mangement in SCADA Systems", **IEEE International Conference,** 150-155, 10-12 Temmuz 2011.

[24] M. Castrucci, ve diğ., "Design and Implementation of A Mediation System Enabling Secure Communication Among Critical Infrastructures", *International Journal of Critical Infrastructure Protection*, 86-97, 2012.

[25] A. Özbilen, **TCP/IP Tabanlı Dağıtık Endüstriyel Denetim Sistemlerinde Güvenlik ve Çözüm Önerileri,** Doktora Tezi, Elektrik Eğitimi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 2012.

[26] V. Urias ve diğ., "Supervisory Command and Data Acquisition (SCADA) system Cyber Security Analysis using a Live, Virtual, and Constructive (LVC) Testbed", **Military Communications Conference**, 1-8, 29 Aralık-1 Kasım 2013.

[27] H. Çiftçi, **Her Yönüyle Siber Savaş**, Tübitak Popüler Bilim Kitapları, Ankara, 2013.

[28] R. A. Clarke, R. K. Knake, **Cyber War – The Next Threat to National Security and What to Do About It,** 2012.