T.C.
İNÖNÜ ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ

BİLGİ TOPLUMU DÖNÜŞÜM SÜRECİNDE E-DEVLET KAVRAMININ SİBER ÜLKE GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

DANIŞMAN HAZIRLAYAN
Yrd. Doç. Dr. Ender AKYOL **Özkan KARAKUZU**

MALATYA - 2015

BİLGİ TOPLUMU DÖNÜŞÜM SÜRECİNDE E-DEVLET KAVRAMININ SİBER ÜLKE GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ

Özkan KARAKUZU

Danışman: Yrd. Doç. Dr. Ender AKYOL

İnönü Üniversitesi Lisansüstü Eğitim-Öğretim Yönetmeliği'nin

SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI İçin Öngördüğü

YÜKSEK LİSANS TEZİ Olarak Hazırlanmıştır.

MALATYA

Nisan 2015

İNÖNÜ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

İnönü Üniversitesi Siyaset ve Sosyal Bilimler Anabilim Dalı Yüksek Lisans Öğrencisi Özkan KARAKUZU'nun hazırladığı "Bilgi Toplumu Dönüşüm Sürecinde E-Devlet Kavramının Siber Ülke Güvenliği Açısından Değerlendirilmesi" başlıklı tez, aşağıda imzaları bulunan biz jüri üyelerince oy birliği~~/oy çokluğu~~ ile başarılı bulunmuştur.

BAŞKAN..Doç.Dr.S.Mustafa ÖNEN.....

ÜYE..Yrd.Doç.Dr.Ender AKYOL (Danışman)..

ÜYE..Yrd.Doç.Dr.Ahmet IVNG.....

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

...../...../ 2015

Prof. Dr. Mehmet KARAGÖZ

Sosyal Bilimler Enstitüsü Müdürü

ONUR SÖZÜ

Yüksek lisans tezi olarak sunduğum "**Bilgi Toplumu Dönüşüm Sürecinde E-Devlet Kavramının Siber Ülke Güvenliği Açısından Değerlendirilmesi**" başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın tarafımdan yazıldığını ve yararlandığım bütün yapıtların metin içi ve kaynakçada yöntemine uygun olarak gösterilenlerden oluştuğunu belirtip, bunu onurumla onaylarım.

….. / ….. / 2015

Özkan KARAKUZU

ÖNSÖZ

Üzerinde çalışmaktan ve araştırma yapmaktan zevk aldığım, bilgi toplumunun ve teknolojik çağın en güncel meselesi olmasına rağmen akademik anlamda üzerinde yeterince çalışma yapılmadığını düşündüğüm siber ülke güvenliğinin E-Devlet kavramı açısından sınanmasını içeren bu tezimin önemli bir çalışma olduğu kanaatindeyim. Bilişim toplumunda devlet uygulamalarının, dolayısı ile devlet örgütlenmesinin, bilgi sistemleri vasıtalarıyla dijital hale getirilmesi sayesinde, devletlerinde güvenlik kavramı değişmeye başlamıştır.

Tarım toplumundan sanayi toplumuna, sanayi toplumundan da bilgi toplumuna dönüşüm süreci devam ederken, devletlerin de bu doğrultuda değişmesi ve dönüşmesi kaçınılmazdır. Bilgi toplumu dönüşümünde elektronik devlet yönetimi olarak karşımıza çıkan E-Devlet uygulamaları, gerek bireysel gerekse organize olmuş suç örgütleri tarafından her geçen gün artan bir oranda siber saldırılara maruz kalmaktadır. Devletler, E-Devlet süreciyle birlikte yönetim ve hizmet sunumu açısından dijital forma dönüşürken, kritik altyapıların ve E-Devlet uygulamalarının güvenliğinin nasıl sağlanacağı hep sorulagelmiştir. Bu kaygılar sebebiyle E-Devletleşme sürecine kuşkuyla yaklaşılmıştır. Bu kaygıların haklılığına ve yapılması gerekenlere bu çalışmamda cevap aramaya çalıştım. Siber güvenlik kavramının yeni bir olgu olması, mevcut basılı kaynakların çok sınırlı olması sebebiyle, çalışmalarımda kitap, makale, dergi, kurum raporu ve internet kaynaklarından yararlandım.

İlerleyen zaman içerisinde yaşanabilecek olası siber saldırılar veya savaşlar sonrasında, siber güvenlik algısının toplum ve devlet nazarında daha da önem kazanacağını düşündüğümden, çalışmamın bu alanda mevcut olan bir boşluğu dolduracağı ve ileriye dönük bir başvuru kaynağı olacağı inancındayım. Tez yazımı süresince bana desteğini esirgemeyen danışmanım Yrd. Doç. Dr. Ender AKYOL'a teşekkür ederim. Tezimi yüksek lisans öğrenimim sırasında ve tez yazım aşamasında, yalnız bıraktığıma inandığım ve oyun zamanından çaldığım biricik oğlum Alper'e adamak istiyorum.

Özkan KARAKUZU

BİLGİ TOPLUMU DÖNÜŞÜM SÜRECİNDE E-DEVLET KAVRAMININ SİBER ÜLKE GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ

Özkan KARAKUZU

İnönü Üniversitesi Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı

Yüksek Lisans Tezi: Nisan 2015

ÖZET VE ANAHTAR KELİMELER

Bu çalışmada, bilişim toplumu dönüşüm sürecinde, kamu yönetiminde bir araç olarak kullanılmaya başlanan E-Devlet kavramının kısaca gelişimine ve özelliklerine değinilmiş, küreselleşme ve gelişen bilgi teknolojilerinde meydana gelen yeniliklere paralel olarak kamu yönetiminde, sürekli erişilebilir, şeffaf, hızlı ve bürokrasiden olabildiğince arındırılmış bir idari yapının kamu yönetiminde görülme isteği belirtilmiştir. Bilgi toplumu dönüşüm süreci içinde değişen kamu yönetimi idaresi algısı da, karar vericileri, bu yeni isteklere cevap verebilme adına, klasik devlet anlayışına nazaran daha iyi çalışan bir idari yapı kurma zorunluluğuna itmiş ve böylelikle E-Devlet kavramı ortaya çıkmıştır. E-Devlet uygulamaları sayesinde sunulan hizmetler kritik altyapıları da kapsayacak şekilde gelişmiş ve bir noktadan sonra olası siber saldırıların ülke güvenliğine zarar verebileceği değerlendirilmiştir. Yakın geçmişte yaşanan siber saldırılardan örnekler verilerek, aslında konunun ne kadar hassas ve önemli olduğunun üzerinde durulmuştur. E-Devletleşme sürecine karşı duyulan kuşkuların bertaraf edilmesi adına, bireysel, kamu kurum ve kuruluşları ve devlet örgütlenmesi adına alınması gereken tedbirler çalışmada yer almıştır. Her ne kadar siber ülke güvenliği kaygısı, E-Devletleşme süreci üzerinde bir baskı unsuru olarak bulunsa da teknolojinin insanoğluna ve kamu yönetimine sunduğu yeni imkan ve kabiliyetlerden vazgeçmek veya bu gelişmelerden geri kalmak mümkün görünmemektedir.

Anahtar Kelimeler: Bilgi Toplumu, E-Devlet, Siber Saldırı, Bilgi Güvenliği, Siber Güvenlik, Siber Savaş.

DURING THE TRANSFORMATION PROCESS OF INFORMATION SOCIETY, EVALUATING THE CONCEPT OF E-GOVERNMENT ON THE BASIS OF CYBER SECURITY OF THE COUNTRY

Özkan KARAKUZU

Master Thesis Submitted to the Department of Public Administration, Social Sciences Institute, Inonu University, Malatya, Turkey, April, 2015

Advisor: Asst. Prof. Ender AKYOL

ABSTRACT AND KEY WORDS

In this study, during the transformation process of information society, the concept of e-government has mentioned briefly with its features. Instead of classical administration, new society's bureaucracy-free, fully accessible, transparent public administration request with the help of globalization and emerging information technologies and innovations, has stated in this study. Changing the perception of the public administration in the process of transformation of the information society, the decision makers to respond to these new demands in the name of the classical conception of the state than the requirement to establish a well-functioning administrative structure, and thus the concept of e-government has emerged. The services offered through e-government applications have developed to include critical infrastructure and at one point it considered as a possible cyber-attacks that could compromise the safety of the country. Some examples of cyber attacks which took place in recent past have given in this study in order to show how sensitive and important the issue. On behalf of to compensate suspicions against e-government process, what kind of measures should be taken for public institutions and government structures has mentioned in this study. Although the concern of cyber security of the country, which is still an element of pressure on the process of e-government, there seems to be no way to give up from the e-government or from its offer to mankind.

Key Words: Information Society, e-Government, Cyber Attack, Information Security, Cyber Security, Cyber Warfare.

BİLGİ TOPLUMU DÖNÜŞÜM SÜRECİNDE E-DEVLET KAVRAMININ SİBER ÜLKE GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ

İÇİNDEKİLER

Sayfa No

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

AB	**:**	Avrupa Birliği
ABD	**:**	Amerika Birleşik Devletleri
BİLGEM	**:**	Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BM	**:**	Birleşmiş Milletler
BTK	**:**	Bilgi Teknolojileri Kurumu
CHA	**:**	Cihan Haber Ajansı
DPT	**:**	Devlet Planlama Teşkilatı
EBYS	**:**	Evrak Bilgi Yönetim Sistemi
ESHS	**:**	Elektronik Sertifika Hizmet Sağlayıcısı
EU	**:**	Avrupa Birliği
GES	**:**	Genelkurmay Elektronik Sistemler
MERNİS	**:**	Merkezi Nüfus İdare Sistemi
MİT	**:**	Milli İstihbarat Teşkilatı
NATO	**:**	Kuzey Atlantik Antlaşması Örgütü
IP	**:**	İnternet Protokolü
ITU	**:**	Uluslararası Telekomünikasyon Birliği
İTO	**:**	İstanbul Ticaret Odası
TASAM	**:**	Türk Asya Stratejik Araştırmalar Merkezi
TDK	**:**	Türk Dil Kurumu
TUİK	**:**	Türkiye İstatistik Kurumu
TÜBİTAK	**:**	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TSK	**:**	Türk Silahlı Kuvvetleri
UEKAE	**:**	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü
YÖK	**:**	Yüksek Öğrenim Kurumu

BİLGİ TOPLUMU DÖNÜŞÜM SÜRECİNDE E-DEVLET KAVRAMININ SİBER ÜLKE GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ

Özkan KARAKUZU

1. ARAŞTIRMA HAKKINDA AÇIKLAMALAR

Bu bölüm, "Araştırmanın Konusu ve Önemi", "Araştırmanın Hipotezleri", "Araştırmanın Amacı", "Araştırmanın Yöntemi", "Bilgi Derleme ve İşleme Araçları", "Kavram Tanımları ve Kuramsal Çerçeve", ve "Araştırmanın Sunuş Sırası" adlı başlıklardan oluşmaktadır ve araştırma konusunu tanıtıcı özet bilgiler içermektedir.

1.1. Araştırmanın Konusu ve Önemi

İnsanlık tarihine bir göz atıldığında toplumsal değişim ve gelişimin çeşitli etkenlerle birlikte, farklı dönemlerde farklı özelliklerle beraber hızla gerçekleştiği görülmektedir. İlkel çağlardan günümüze bilgi ve teknoloji, toplumsal gelişmenin temel itici gücü olmuştur. Daha ilgi çekici olanı ise 1950'lerden sonraki teknolojik gelişmeler bütün insanlık tarihindeki teknik oluşların hemen hepsinden daha fazla ve hızlıdır. Tarih öncesi ilkel insan, ateşin buluşundan, pişirilmiş tuğlaya bin yılda geçebilmiştir. Pişkin tuğladan ilk buhar makinesine geçiş ise on bin yılda gerçekleşmiştir (Tunaya, 1980: 4). Sonraki elektrik, uzay teknolojileri, atom enerjisi, bilgisayar, internet, nano-teknoloji vs… gibi gelişmeler içinse, ne on bin yıl ne de onlarca yıl beklemek gerekmektedir. Teknoloji baş döndürücü bir hızla gelişmekte ve insanlığı şaşkına çevirmektedir.

Bu gelişmelere paralel olarak, bilgi toplumu dönüşüm sürecinde, kamu yönetimi algısı ve anlayışı da derinden değişmektedir. Bu gelişim ve değişim, ülke güvenliğini de yakından etkilemektedir. Devlet ile toplum arasındaki yönetim açısından birçok yenilik ve farklılık getiren E-Devlet kavramının gelişimi, amaçları ve getireceği faydalar ile E-Devletleşmenin, siber ülke güvenliği bağlamında incelenmesi/irdelenmesi araştırmanın konusunu oluşturmaktadır. Kamu yönetimi açısından devlet idaresine, kamu hizmeti alımı açısından ise toplum nezdinde, E-Devlet sürecinin neler getirdiği ve getireceği, ne tür fayda ve yararlarının olacağının irdeleneceği araştırmada, siber güvenlik kaygısının E-Devletleşme sürecine etkisi ve ülke güvenliği açısından incelenmesi de

hedeflenmektedir. Bu çalışmayla birlikte E-Devlet kavramının siber ülke güvenliğine fayda ve zararlarının ortaya konulması amaçlanmaktadır.

Her türlü bilginin ve verinin dijital olarak muhafaza edildiği E-Devletleşme sürecinde, dijitalleşen kamu hizmetlerinin siber saldırılara maruz kalması halen sıklıkla karşılaşılan bir olgudur. Araştırma konusunun, E-Devletleşme karşısında önemli bir engel olan siber güvenlik konusunu işliyor olması sebebiyle, Kamu Yönetimi Ana Bilim Dalı açısından önemli olduğu değerlendirilmektedir.

1.2. Araştırmanın Hipotezleri

Araştırmanın konusu, önemi ve amacı ile oluşturulan çerçeveye bağlı kalınarak, araştırma boyunca sınanacak olan hipotezler aşağıda belirtildiği gibidir.

Hipotez 1: Küreselleşen dünyada, her geçen gün değişen ve daha karmaşık hale gelen kamu yönetimi, bilgi toplumu dönüşümü süreci içerisinde, gelişen bilgi teknolojilerinden de yararlanarak, E-Devlet kavramıyla tanışmıştır. Yeni devlet yapısı yönetiminin etkin, şeffaf, faydalı ve verimli hizmetler sunabilmesi amacıyla, kamu yönetiminde E-Devletleşme süreci kaçınılmazdır.

Hipotez 2: Siber güvenlik algısı ve bunun getirdiği tehditler E-Devlet kavramının gelişmesine, yayılmasına ve derinleşmesine zarar vermektedir. Günümüz bilgi teknolojilerinin imkân ve kabiliyetleriyle gelişen ve gelişmekte olan E-Devlet olgusunun önündeki en büyük engel siber ülke güvenliği kaygısıdır.

Hipotez 3: Siber ülke güvenliği, en alt birimden en üst seviyeye kadar alınabilecek önlemler ile sağlanabilmekte veya alınan önlemlerle olası bir siber saldırının, ülke güvenliğine olan tesiri ve etkisi en aza indirilebilmektedir.

1.3. Araştırmanın Amacı

Son yıllarda bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmeler hayatımızın her yönüne etki etmekte ve bu etki gün geçtikçe artmaktadır. Günümüzün sloganı olan "Bilgi güçtür!" deyimi artık her alanda kullanılır olmuştur. Gelişen bilgi teknolojileriyle

birlikte vatandaş-devlet ilişkisi de yeni bir boyut kazanmaktadır. 1990'lı yıllardan itibaren internet kullanımının ve internete erişim imkânlarının hızla artması ve tüm dünyada yaygınlaşmasıyla birlikte, elektronik ticaretin yaygın olarak kullanıldığı yeni bir piyasa anlayışının ortaya çıktığı görülmektedir. Elektronik ticaretin, klasik ticaret ve piyasa anlayışına nazaran, gerek zaman ve gerekse maliyet açısından daha ekonomik, etkin ve hızlı olması, bu kavramın farklı bir boyutta kamu yönetimine uyarlanmasını gündeme getirmiş ve böylece E-Devlet kavramı literatürde yerini almıştır.

Ülkeler elektronik ticaretin üstünlüklerini fark edip, devlet yönetimini özel sektör gibi daha etkin ve verimli hale getirme gayreti içerisine girmişlerdir. Bu çaba içerisinde üzerinde durulan en önemli olgu E-Devlet kavramıdır. E-Devlet kavramı, küreselleşen dünyada, her geçen gün değişen ve daha karmaşık hale gelen kamu yönetiminin, gelişen bilgi teknolojileri ve bilgi toplumu algısı içerisinde dönüşmesi sonucu ortaya çıkmıştır. Gelişen E-Devlet yapısı, çoğu kamu hizmetini kesintisiz hizmet verilebilir hale getirmiştir. E-Devlet uygulamaları ve servisleri, bir taraftan bürokrasiyi azaltırken, diğer taraftan sunmuş olduğu hizmetlerle ilgili çoğu bilgiyi elektronik ortamda muhafaza etmektedir. Sürdürülen bu E-Devlet hizmetlerinin, ülke kurum/kuruluşları ve vatandaşları için sayısız faydaları olmasına rağmen, hassas nitelikte olabilecek çoğu bilgi ve belgeyi siber saldırılara açık hale getirmesinden dolayı siber güvenlik tehlikesi yaşanmaktadır. Birtakım yollarla yapılan bu saldırılar sonucu kamu kurum ve kuruluşlarının E-Devlet uygulamaları hizmet veremez hale gelmekte veya hizmetin kalitesi düşmektedir.

Günümüz bilgi teknolojilerinin imkân ve kabiliyetleriyle gelişen ve gelişmekte olan E-Devlet olgusunun önündeki en büyük engel siber ülke güvenliği endişesi ve bilinmezliğidir. Ülkeler halen gelişmekte olan bu siber dünyaya karşı ne kadar kırılgan olduklarını bilmediklerinden, hizmet sunumunda, teknolojinin imkanlarından sonuna kadar yararlanılamamaktadır. Meydana gelen siber saldırılar ülkeleri E-Devletleşme yolunda endişeye sevk etmektedir. Araştırmamın amacı, E-Devletleşmeyle dijital hale gelen kamu hizmetlerinin, siber saldırılar neticesinde gerçekten hizmet dışı bırakılıp bırakılamayacağını sorgulamak, kesintisiz bir E-Devlet hizmet sunumu yapabilmek için bireysel, kurumsal ve devlet yönetimi bazında alınması gereken tedbirleri sıralamaktır. Ortada mevcut bir tehdidin yaşanan olaylar ışığında derecelendirildiği bu çalışmada olası sonuçlar ve nasıl bertefar edilebileceği üzerinde durulmuştur. Meydana gelen siber

saldırılar ve bilinen etkileri doğrultusunda, bir durum tespiti yapmak, sonucunda ise hipotezlerimi sınayarak çalışmamı sonuçlandırmayı amaçladığım bu çalışma, alanında E-Devletleşme ile siber ülke güvenliğini irdelemesi bakımından bir boşluğu dolduracağını düşünmekteyim. İşte tam bu noktada kamu yönetimi anlamında her geçen gün daha fazla kullanım alanı bulan E-Devlet kavramının, siber ülke güvenliği kaygısı ve olası sonuçlarıyla analiz edilmesi, araştırmanın ana amacını oluşturmaktadır.

1.4. Araştırmanın Yöntemi

Araştırma dört kesim yaklaşımına göre hazırlanmış ve toplam altı bölümden oluşmaktadır. Bu tez, betimleyici araştırma tasarımıyla kurgulanmış, durum saptaması yapan bir çalışmadır. Araştırmada kapsamlı literatür çalışması ve kaynak taraması yapılacak olup, kavramsal bölümün ardından üçüncü kesimde hipotezler sınanacak ve elde edilen sonuç ve öneriler dördüncü kesimde belirtilecektir. Bu çalışmada kullanılan veri toplama tekniklerinden kaynak tarama tekniği kapsamında birçok akademik kitap, dergi ve web sitesi taranmış olup, konuyla ilgili mevcut yazılı kaynaklarla birlikte, kamu veya özel kurum raporları incelenmiş, açık kaynak bilgilerden de yararlanılmıştır.

1.5. Bilgi Derleme ve İşleme Araçları

Araştırmanın birinci kesimini, "Araştırma Hakkında Açıklamalar" başlığı altında, araştırma hakkında tanıtıcı bilgiler oluşturacaktır. İkinci kesimi ise "Bilgi Toplumu Kavramı ve Bilgi Toplumu Dönüşüm Süreci", "Değişen devletin rolü, E-Devlet ve E-Devleti Gerekli Kılan Nedenler" ile "Bilgi Güvenliği ve Siber Güvenlik Kavramı" başlıkları oluşturacaktır. Üçüncü kesimde ise "Siber Ülke Güvenliği Kaygılarının E-Devletleşme Sürecine Etkisi ve Alınması Gereken Tedbirler" başlığı altında hipotezler sınanacaktır. Araştırmanın dördüncü ve son kesimi olan "Genel Değerlendirme" de Bulgular, Öneriler ve Genel Sonuç açıklanacaktır.

Araştırmada, konu başlıkları hakkında yazılı ve görsel medyada yayımlanmış çeşitli kitaplar, makaleler, tez çalışmaları, internet kaynakları taranacak ve elde edilen bilgiler araştırmacının eklemeleri ile özgün olarak derlenecektir. Araştırmanın genel

değerlendirme ve sonuç bölümünde elde edilen bilgiler ışığında, araştırmanın konusunun çözümlenmesi planlanmaktadır.

1.6. Kavram Tanımları ve Kuramsal Çerçeve

Bu bölümde araştırma içerinde incelenecek olan temel kavramlardan "Bilgi Toplumu", "E-Devlet", "Küreselleşme Kavramı", "Siber Uzay" ile "Siber Güvenlik" kavramları sırasıyla açıklanmıştır.

1.6.1. Bilgi Toplumu Kavramı

Bilgi toplumu üzerine yapılan çalışmalarda, bilginin niceliksel ve niteliksel artışının yaşanan teknolojik gelişmelerle birlikte, ekonomiden politikaya, sanattan kültüre, tüm alanlarda öneminin arttığı ve artmaya devam edeceği beklentisi belirgindir. Bu beklentilerin oluşmasını sağlayan en büyük etken, bilginin temel üretim faktörü durumuna gelmesi, emek ve sermayenin öneminin ise giderek azalmasıdır. Bu bağlamda sanayi toplumuna özgü klasik emek-sermaye çelişkisinin çözülerek, yeni bir toplumsal yapının oluşmasını sağlayacak, yeni ilişkilerin ortaya çıkacağı varsayılmaktadır.

Bu yaklaşım paralelinde bilginin, sermaye, hammadde, enerji ve insan gücü gibi üretim unsurlarından biri haline dönüştüğü, ekonomide hammadde ve ürün olarak kullanıldığı, herkes tarafından paylaşıldığı ve toplum içerisinde kültürel bir değer olarak kabul edildiği ve bilgi-iletişim teknolojilerinin her alanda kullanılmaya başlandığı topluma Bilgi Toplumu denir (Rukancı ve Anameriç, 2004). Bilgi toplumunu; yeni temel teknolojilerin gelişimiyle, bilgi üretiminin, bilgi sermayesinin ve nitelikli insan faktörünün önem kazandığı, iletişim teknolojilerinde yaşanan yeni gelişmeler sayesinde toplumu ekonomik, sosyal, kültürel ve siyasal açıdan sanayi toplumunun ötesine taşıyan bir gelişme aşaması olarak tanımlamak da mümkündür. Bilgi toplumunda, bilgi anlamlı tek kaynak olarak benimsenmekte; geleneksel üretim faktörleri yani doğal kaynaklar, emek ve sermaye ortadan kalkmamakta ancak, ikinci plana düşmektedir. Söz konusu üretim faktörleri, bilgi sayesinde elde edilebilir kaynaklara dönüşmektedir. Toprak ve sermayenin temel üretim girdisi olmaktan çıkması, bunların yerine bilginin "temel

üretim girdisi" olduğu toplumsal yapı, bilgi toplumu olarak tanımlanmakta ve nitelikli bilgi önem kazanmaktadır. Bilgiyi kullanacak olan insandır. Dolayısı ile bilgi toplumunda diğer önemli girdi insan faktörü olmaktadır. Burada, düşünsel anlamda emek faktörünün gelişimi, insana yapılacak yatırımları ön plana çıkmaktadır (Aktan ve Tunç, 1998: 118-134).

Bilgi toplumu özellikle rutin, mekanik ve tekrara dayanan işlemleri yıkmaktadır. Bu işlemlerin yerine bireylerin yaratıcılığına ve duygusal zekâlarına dayanan işlemlere geçilmekte ve böylelikle toplumun yaşam kalitesi de yükselmektedir. Bilgiyi yaratmak, var olan bilgiyi yorumlamaktan daha öte bir anlayıştır. Var olan bilgiyi yorumlamak teknik bir boyut iken bilgi yaratmak için hayal gücü, sezgi ve içgüdüden yararlanmak gerekmektedir. Tarım toplumu, sanayi toplumu ve bilgi toplumu eksenine göz attığımızda tarım ve sanayinin bu toplumların temelini oluşturan üretim süreçleri ile doğrudan bağlantısı göze çarpar. Oysa bilgi toplumunda üretim doğrudan bilgi kullanımı ile değil; bilgi kullanımıyla zenginleştirilmiş ve etkinleştirilmiş bir şekilde, ama yine tarım ya da sanayi üretim şekillerinden birinde olmaktadır. Bu nedenle Bilgi Toplumu derken kastedilenin "bilgi temelli toplum" ya da "bilgi güdümlü toplum" olduğu gözden kaçırılmamalıdır (Tekman, 2002: 265-266).

Yeni teknolojik imkanlar sayesinde, insanoğlu edindiği bilgiyle fiziksel engelleri aşarak, ülke sınırlarının da ötesinde global marketlere, erişebilmiştir. Modern iletişim sistemleri, bilgiyi çok uzaklardan anlık olarak temin edip hızlı karar verebilmemizi mümkün hale getirmiştir. İnternetin ve mobil iletişim sistemlerinin gelişmesi, uluslararası ticareti erişile bilinir kılmış, yerel üreticilerin global piyasayı takip ederek ürün ve hizmetlerini geliştirmelerini mümkün hale getirmiştir. Meydana gelen uluslararası standartlardaki değişimin ürünlere uygulanabilirliği hızlı ve zamanında olmuş, bu da toplumun bu değişimi kabullenmesine ve giderek artan oranda dijitalleşmesine çanak tutmuştur. Bireysel ve kurumsal anlamdaki kazançlarının yanında, devlet yönetimi olarak, bu yeni gelişmekte olan bilişim toplumu, yatırımcıların hızlı kararlar almasına, dolayısı ile kişi başı gelirin artmasına, ihracat ürünlerinin kalitesinin hızla uluslararası standartlara ayak uydurması neticesinde ülke olarak piyasa standartlarının hızla yakalanıp rekabetten kopmamak adına faydalar sağlamıştır. (Shishkov, 2014: 273-274).

Bilgi toplumunda, bilgi, üretimin merkezinde yer almaktadır. Bilginin çalışma hayatına, çalışma şekline, bireylere, ekonomiye ve devlet yönetimine dolayısı ile toplumun geneline etkisi bulunmaktadır. Bilgi gereksinimi ve ihtiyacı, bir süre sonra yerini nitelikli ve teknik bilgi ihtiyacına bırakmakta, bu da toplumun ve bireyin daima yeni ve yaratıcı bilgiler ışığında gelişmesi ve dönüşmesini getirmektedir. Giderek artan bir şekilde nitelikli bilgiye olan ihtiyaç, bu bilgiye haiz nitelikli insan ihtiyacını da beraberinde getirmektedir. Bilgi toplumunda bilginin üretilmesi ve kullanımında, sanayi toplumunun aksine insan birincil roldedir (Vukasinovic, 2014: 476-479).

Ağ toplumu olarak da adlandırılan bilgi toplumunun, ekonomiden, sanayiye, eğitimden sağlığa farklı alanları bulunmaktadır. Toplumu ilgilendiren hemen her alanda yaşanan gelişmeler, bilgi ekseni etrafında toplumu başka bir noktaya taşımıştır. Henüz tam olarak uyum sağlayamadığımız bu yeniçağ, bilgi çağıdır. Teknolojinin itici gücüyle yeni buluş ve gelişmelerin ışığında ilerleyen bu bilgi toplumuna dönüşüm süreci toplumu şekillendirmeye devam etmektedir (Miles, 2004: 2-7).

1.6.2. E-Devlet Kavramı

Klasik devlet anlayışının getirdiği bürokratik yapıdan dolayı hantallaşan devlet yapısı, artık toplumun ihtiyaçlarına ve gereksinimlerine cevap veremez hale gelmiştir. Devletler bilgi ve iletişim teknolojilerinin avantajlarından yararlanmak için dijitalleşmekte ve böylelikle hizmet kalitelerini iyileştirmeyi hedeflemektedirler. Artık teknolojinin ve bilişim sistemlerinin sunduğu avantajlar hizmetlerin daha kolay ve hızlı sunumunu mümkün hale getirmiştir (Büke, 2002: 12).

E-Devlet, gündelik yaşamda çok sık kullanılmasına rağmen, ne ifade ettiği hakkında çok az bilgi veya fikir sahibi olunan bir kavramdır. Bunun nedeni; E-Devlet kavramının somut bir temele oturmaması ve toplumda bu kavramın farklı düşünceler çağrıştırması olarak açıklanabilir. E-Devlet kavramının birçok tanımı yapılmıştır. Bu tanımların temel ortak noktası, devlet işlerinin elektronik ortamda yapılmasıdır. Bu bağlamda, E-Devlet, kamu kurum ve kuruluşları, devlet organlarıyla yapılan her türlü işlemin, servis veya hizmetin uygun bilişim teknolojileri kullanılarak, elektronik ortamda sürdürülmesi olarak tanımlanmaktadır (Emiroğlu, 2003).

Türkiye Bilişim Derneği'nin "E-Devlet Yolunda Türkiye" çalışmasında E-Devlet kavramı; "Devletin vatandaşlara karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile vatandaşların buna karşılık devlete karşı olan görev ve hizmetlerin karşılıklı olarak elektronik iletişim ve işlem ortamlarında kesintisiz ve güvenli olarak yürütülmesidir" şeklinde açıklanmıştır (Arifoğlu vd., 2002: 12). Tanımlardan da anlaşılacağı gibi E-Devlet sayesinde, temel olarak kamunun hizmet verdiği alanlarda, bilgi ve iletişim teknolojilerinin kullanılması yoluyla daha şeffaf, vatandaşa daha yakın, daha hızlı ve daha iyi çalışan bir idari yapı oluşturulması amaçlanmaktadır (İnce, 2001: 21).

E-Devlet temel anlamda gerçek hayattaki devletin, teknoloji olanaklarını kullanarak çağın gereklerine uygun olarak yeniden yapılandırılmasıdır (www.milliemlak.gov.tr, 17.08.2013). E-Devlet, kullanıcılara mevcuttan daha fazla bilgiye ve kaynağa daha hızlı bir şekilde ulaşma imkânı sağlamaktadır. Oluşturulan elektronik ortamla, birey geçmişe ve bugüne ait bilgilerin yerini öğrenmekte, ortaya çıkarmakta, böylece yeni bilgilere ulaşmakta ve bu bilgileri kullanarak her hangi bir kuruma gitmeksizin elektronik ortam üzerinden hizmet almakta, işlem yürütmektedir (Ulusoy ve Karakurt, 2002: 135). Kamu bilgilerine ulaşma olanağı, elektronik devletin sadece bir yüzüdür. Elektronik devlet, vatandaşların bilgiye erişme taleplerini karşılamakla kalmamakta, ayrıca kamu hizmetlerinin elektronik yapılar içinde yürütülmesini ve vatandaşların kendileri hakkındaki bilgileri sorunsuz ve kolay bir şekilde, konuyla ilgili birimlere aktarılmasını da içermektedir (Mutioğlu, 2002: 962).

Devletin temel unsurları olan vatandaş ve kurumlar E-Devlette, e-vatandaş, e-kurum ve e-şirket şeklinde ortaya çıkmaktadır. Vatandaş, kurum ve işletmenin E-Devletteki anlamları şöyledir:

e-vatandaş; devletle olan iletişim ve bağlantısını bilgisayar ağları üzerinden gerçekleştiren yurttaştır.

e-kurum; vatandaşa bilgisayar ağları üzerinden, dijital ortamda hizmet sunan kurumdur.

e-şirket; çevreyle olan iletişimini ve işlemlerini bilgisayar ağları üzerinden yapan şirketlerdir (Şahin ve Örselli, 2003).

E-Devletleşme süreciyle devlet yönetimleri, vatandaşlara karşı daha şeffaf ve erişilebilinir hizmet sunmakta ve böylelikle yönetimlerin reaksiyon süresi kısalmaktadır. E-Devlet hizmetlerinin sunulduğu ülkelerdeki ekonomilerde yolsuzluk oranları düşmekte hatta çoğu alanda yolsuzluğun önüne geçilebilmektedir. Hizmet servislerinin E-Devlet uygulamalarıyla yönetildiği devlet yönetimlerinde hizmet kalitesi artmakta, yoksulluk azalmaktadır. Çoğu olumlu faydası neticesinde Vatandaş-Devlet Yönetimi ilişkisi de, E-Devlet sayesinde kuvvetlenmektedir (Ionescu, 2015: 48-53).

E-Devlet uygulamaları, yoğun olarak internet ve bilgi teknolojilerini kullanmaktadır. E-Devletleşme süreci başlıca dört ana safhadan oluşmaktadır. Bunlar; Bilgi Edinme, Etkileşim, İşlem ve Entegrasyon aşamalarıdır. E-Devletleşme herşeyden önce elde bulundurulan bilginin hızlı bir şekilde gerektiğinde hizmet talep edenlere ulaştırılması sürecidir. Bu safha "Bilgi Edinme" olarak adlandırılmaktadır. Bilgiye erişim sonrasında, onu değerlendirme yani "Etkileşim" safhasına geçilmektedir. E-Devletleşme sürecinin üçüncü safhası ise, bu değerlendirilen bilgi veya verinin istenilen hizmete ve amaca yönelik işlenmesi/kullanması aşaması olan "İşlem" safhasıdır. Son olarak işlenen bu verinin/bilginin neticesinde, elde edilen hizmet veya ürün "Entegrasyon" safhasında nihayi formuna dönüştürülerek kullanıcının talebini karşılamış olmaktadır (Mellouli, 2014: 283-285).

1.6.3. Küreselleşme Kavramı

1989 yılında özellikle doğu blokunun dağılması ve ardından 1991 de Sovyetler Birliği'nin yıkılması ile birlikte, küreselleşme olgusu yirminci yüzyılın son çeyreğinde kendisini fazlasıyla hissettirmiştir (Eken, 2006: 246-247). İletişim çağı, küresel köy, sanayi sonrası toplum gibi pek çok kavram tarihsel olarak 1900'lerden önce ortaya atılmıştır. Çok boyutlu bir kavram olan küreselleşmeyi kısaca tanımlayacak olursak; Mal, hizmet, sermaye ve bilginin ulusal sınırları kolaylıkla aşması bütün dünyayı engelsiz bir biçimde dolaşması ve "zaman-mekân farkının etkisini yitirmesi" dünyanın "tek bir yer" olma sürecinin belirgin özellikleri olarak belirtilebilir. Teknolojik alanda kaydedilen ilerlemeler sayesinde bilgiye erişim hızla gerçekleştirilebilmekte, toplumsal sistem ekonomiyle beraber değişime uğramaktadır (Akgün, 2003: 57).

Küreselleşme kavramının yasal, teknolojik, yönetimsel, ekonomik, sosyal ve kültürel birden fazla boyutu mevcuttur. Ekonomik anlamda küreselleşme, tek ve bütünleşmiş bir dünya pazarı olarak gelişmekte iken, siyaset bilimi açısından incelendiğinde ulus devletten ayrılarak bölgesel egemenlik kavramının ön plana çıktığı, çok uluslu şirketlerin söz sahibi olduğu yeni bir dünya düzeni olgusu algılanmaktadır. Küreselleşme, özünde ileri teknolojiye ve kapitalizme dayalı bir ekonomi politikasıdır. Küreselleşmenin yarattığı etki sonucunda, dünya genelinde fikirler, düşünceler, teknolojiler, sermaye ve bilgi, ulus-devlet sınırlarını aşmış ve böylelikle mesafeler yakınlaşmış, dünya, erişim anlamında küçülmüş, rekabetin boyutu artık ülke sınırlarının dışına çıkmıştır. İletişim teknolojilerindeki gelişmelerin öncülük ettiği küreselleşme sürecinde, ulusal sınırlar anlamını yitirmekte, sermayenin küresel boyutta egemenliği güçlenmektedir (Fedai, 2011: 54-57).

Küreselleşme, bölgesel seviyeninde üstünde dünya ekonomileriyle hızlı bir bütünleşme gerektirir (Murshed, 2002: 1-3). Dünya medeniyetleri ile artan bir hızda etkileşime girme sürecidir. Sınırları ortadan kalkmış bir dünya vadetmektedir. Ekonomik hayata, politik ilişkilere, çevreye, doğaya ve sosyo kültürel yaşama doğrudan bir etkisi olmasına rağmen, ana etkisini ekonomi ve ticarette göstermektedir (Debrah, Y., ve I. Smith, 2001: 2-3).

Sonuç olarak küreselleşme kavramı, çeşitli faktörlerin etkisiyle, sosyal, kültürel ve ekonomik anlamda coğrafi sınırların kalktığı veya önemini yitirdiği, mal ve hizmet ticaretinin arttığı, küresel sermaye hareketinin serbestleştiği, teknolojik yeniliklerin hız kazandığı, böylelikle dünya ekonomisinin bütünleştiği bir süreçtir (Erdut, 2003: 1-2).

1.6.4. Siber Uzay Kavramı

Bilgi toplumu dönüşümü süreciyle birlikte internet, hayatımızın ve çalışmalarımızın vazgeçilmez bir parçası olmuştur. Küreselleşen dünyamızda, küreselleşmenin hızına internet önemli bir katkı sağlamıştır. E-ticaret, e-posta, e-demokrasi, e-medya, e-eğitim, e-sağlık ve E-Devlet gibi kavramlar internet sayesinde hayatımıza girmişlerdir. Siber uzay kavramı da hayatımıza teknolojik gelişmelerin sonucunda giren kavramlardan bir tanesidir. Amerikan Savunma Bakanlığınca siber uzay kavramı "İnternetin bulunduğu, telekomünikasyon ağları ve bilgisayar sistemlerini

de kapsayan, birbirine bağlı bilişim teknolojileri alt yapılarının olduğu küresel bir alan" olarak tanımlanmıştır Daha geniş bir tanımlama ile siber uzay dijital hale getirilmiş bilginin bilgisayar ağları üzerinden iletişime sokulduğu kavramsal ortamı ifade etmektedir (Bakır, 2012).

Siber uzay, metrik olarak ölçülemez. 1980'lerin sonundan itibaren, tıpkı uzaydaki cisimlerin zahmetsiz bir şekilde bir yerden bir yere gitmesinden esinlenilerek, bilginin elektronik ortamda, çeşitli cihazlar üzerinden bir noktadan başka bir noktaya iletilmesinde kullanılan elektronik ortama, siber uzay denilmeye başlanmıştır. Veri iletişiminde kullanılan bilişim sistemleri, (ağ bağlantı cihazları, bilgisayarlar, donanımsal ürün ve cihazlar) siber uzayın görünür araçlarıdır. Siber uzay, insanların çalıştığı, sosyalleştiği, arkadaşlık ilişkileri kurduğu, yeni beceriler öğrendiği ve değişik tecrübeler yaşadığı, kendine has disiplinleri olan bir dünyadır (Mihalache, 2002: 293-300).

1.6.5. Siber Güvenlik

Siber güvenlik, esas itibariyle siber saldırılara karşı alınan tedbirlerin bütününe verilen addır. Kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla geliştirilen politika ve uygulamalar, kullandığı araçlar, yazılı dökümanlar, elektronik ortamda muhafaza ettikleri belgeler ve bilişim alanında kullanılan güvenlik teknolojilerinin tamamı siber güvenliğin unsurları arasındadır. Siber tehdit ve saldırıya maruz kalan bir ülke veya şirket, bu tehdit ve saldırıları bertaraf etmek için siber savunma yapar (Alkan vd., 2012: 11).

Ülkeler, siber saldırı sonucunda zarar görecek kritik altyapılarını, zarar görmesi veya yok olması toplumsal düzenin ve kamu hizmetlerinin devamlılığının sağlanmasında güçlük yaratacak sistem ve uygulamalarını korumak amacıyla, siber savunma yöntemlerini kullanırlar. Kritik altyapılar, erişiminin veya servis hizmetinin engellenmesi durumunda yapısal, ekonomik ve toplumsal anlamda sıkıntı yaşatacak servis ve hizmetlerdir (Henrie, 2013: 38-39).

E-Devlet hizmetlerinin her geçen gün artarak gelişmesi sonucunda, başta kamu olmak üzere çoğu kurum ve kuruluşlar hizmetlerini internet ortamında sunmaya başlamışlardır. Sistem ve hizmetlerin aktarıldığı bu sanal ortamda yaşanacak

olumsuzlukların kişisel, sosyal ve ekonomik hayatımızı önemli ölçüde etkilediği ve etkileyeceği değerlendirilmektedir. Ülkeler tarafından yerinde ve zamanında gerekli siber güvenlik tedbirleri alınmadığı takdirde, gelecekte yaşanabilecek olumsuzlukların daha da artacağı ve oluşabilecek siber saldırıların, hem maddi hem de manevi zararlar vereceği değerlendirilmektedir. Bu siber saldırıların E-Devlet süresince daha da hassas hale gelen bilgi ve belgeleri etkileyerek ülke güvenliğini tehdit edeceği aşikârdır. Siber ülke güvenliğini kamu ve özel sektör anlamında tesis edebilmek için ilgili tüm kurum ve kuruluşlara önemli görevler düşmektedir. Bunların nasıl ve hangi şekilde uygulanabileceği araştırmanın devamında açıklanmıştır (Alkan vd., 2012: 10-13).

1.7. Araştırmanın Sunuş Sırası

Araştırma dört kesim yaklaşımına göre hazırlanmış ve toplam altı bölümden oluşmaktadır. Araştırmanın birinci kesiminde "ARAŞTIRMA HAKKINDA AÇIKLAMALAR" başlığı ile araştırmayı tanıtıcı bilgiler sunulmuştur. Araştırmanın birinci kesimi bir bölümden oluşmaktadır ve bu bölüm "Araştırmanın Konusu ve Önemi", "Araştırmanın Hipotezleri", "Araştırmanın Amacı", "Araştırmanın Yöntemi", "Bilgi Derleme ve İşleme Araçları" , "Kavram Tanımları ve Kuramsal Çerçeve" ve "Araştırmanın Sunuş Sırası" alt bölümlerinden oluşmaktadır.

Araştırmanın ikinci kesimi "Bilgi Toplumu Kavramı ve Bilgi Toplumu Dönüşüm Süreci" ile "Devletin Değişen Rolü, E-Devlet ve E-Devleti Gerekli Kılan Nedenler" bölümlerinden oluşmaktadır. İkinci kesimde bilginin tanımı, özellikleri sonrası, bilgi toplumu dönüşüm sürecine değinilmiş ve E-Devlet kavramının nasıl oluştuğu, vatandaşlara, kurum ve kuruluşlar ile devlet yönetimine sağlayacağı faydalar üzerinde durulmuştur. Geleneksel Devlet - E-Devlet karşılaştırılmasıyla ikinci kesim sonlandırılmıştır.

Araştırmanın üçüncü kesimi "Bilgi Güvenliği ve Siber Güvenlik Kavramı" ile "Günümüzde Başlıca Siber Saldırı Örnekleri" başlıklarından oluşmaktadır. Üçüncü kesimde bilgi güvenliği kavramı, bilgi güvenliği yöntemleri ve tedbirleri açıklandıktan sonra siber güvenlik kavramı irdelenmiştir. Yine üçüncü kesimde siber güvenlik adına dünyada atılmış adımlar incelendikten sonra siber savaş olgusu açıklanmış ve meydana gelen önemli siber savaş ve saldırılardan örnekler verilmiştir.

Araştırmanın dördüncü ve son kesimi, "Siber Ülke Güvenliği Kaygılarının E-Devletleşme Sürecine Etkisi ve Alınması Gereken Tedbirler" ile çalışma boyunca elde edilen bulguların, önerilerin ve genel sonucun bulunduğu "Genel Değerlendirme" başlıklarından oluşmaktadır. Bu bölümde araştırma sonucunda elde edilen bulgular ve bu bulgulara getirilen öneriler ile siber güvenlik kaygısının E-Devletleşme sürecine etkisi ve siber güvenliğin sağlanması amacıyla alınması gereken tedbirler belirtilmiştir. Araştırmanın en sonunda araştırma boyunca yararlanılan kaynakların listelendiği kaynakça bulunmaktadır.

2. BİLGİ TOPLUMU KAVRAMI VE BİLGİ TOPLUMU DÖNÜŞÜM SÜRECİ

Bu bölümde "Bilgi ve Bilginin Tanımı", "Bilgi'nin Özellikleri", "Toplumsal Dönüşüm Süreçlerinin Aşamaları ve Bilgi Toplumuna Geçiş" ve "Bilgi Toplumu Kavramı" incelenmiştir.

2.1. Bilgi ve Bilginin Tanımı

İnsanoğlunun tarih boyunca daha iyiyi bulma arzusu, kendisine sahip olduğu bilgiyi, teknolojiyle destekleyerek geliştirmesine ve yeni imkânlar kazanmasına yol açmıştır. Bilginin tartışılması milattan önce beşinci yüzyılda, felsefeci Sokrates'in bilginin sınırları sorusu ile başlamış (Malhotra, 1997: 241) ve insanoğlu tarafından günümüze kadar tartışıla gelmiştir. Bilgi, çok farklı şekillerde tanımlanmaktadır. Türkçe sözlük anlamı olarak Bilgi: "İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bilim, malumat, öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, insan usunun kapsayabileceği olgu, gerçek ve ilkelerin tümüne verilen ad" şeklinde tanımlanmaktadır (www.tdkterim.gov.tr, 20.12.2012).

Diğer kaynaklarda ise bilgi, daha farklı şekillerde tanımlanmaktadır. Bu tanımlardan bazılarına değinecek olursak, bilgi; öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat ve kavrayışın tümüdür. Bilgi doğruluğu ispatlanmış inançlardır. Bilgi, önceden belirlenen bir dizi sistematik kural ve prosedüre uygun bir biçimde işlenmiş enformasyondur. Bilgi, sosyal varlık olan insanlar

arasındaki iletişim sırasında paylaşılan, aktarılan ve yeniden şekillendirilen tecrübe ve enformasyonlardır (Aktan, 2005).

Bilgi insanlık tarihinin başlangıcından bu yana, değişik dönemlerde farklı önem dereceleri ile değerlendirilmiştir. Başlangıçta salt doğa üzerine bilgi önemli iken, sonraları teknik bilgi öne çıkmıştır (İnce, 2001: 4).

İnsanoğlunun her yetmiş senede, evrenin oluşumundan bu güne kadar edinmiş olduğu toplam bilgiyi ikiye katlandığı ve insanlığın edinmiş olduğu bilginin %90'ının son 30 yılda üretildiği, eğer bilgi sürdürülebilir bir şekilde insanın evrende var olabilme kapasitesi olarak tanımlanırsa o zaman bilginin %90'nının son 30 yılda kaybolduğundan bahseden yazarlar da bulunmaktadır (Erkan, H., ve C. Erkan, 1998: 146).

Bilgi kelimesinin ingilizce karşılığı olarak "data, knowledge" kullanılmaktadır. İşlenmiş veri olarak da tanımlanabilecek bilgi, bir konu hakkında var olan belirsizliği azaltan veya gideren bir kaynaktır (Sağıroğlu, 2013: 9).

2.1.1. Bilgi'nin Özellikleri

Kişi, kurum ve devletler için önemli ve değerli olan bilgi, sürekli gelişen, hareketli ve değişken, işlenmiş bir veridir. Kısaca bilginin özelliklerine değinecek olursak;

- Bilgi işlenmiş bir veridir,
- Bilgi, bir sorunun çözümü için verilen cevaptır,
- Bilgi aynı anda birden fazla yerde olabilir,
- Bilgi sürekli bir değişim içerisindedir,
- Bilgi yaşam için gereklidir,
- Bilgi zamanda ve evrende yer kaplar,
- Bilginin hareketi gürültüsüz ve sessiz olmaz,
- Bilginin hareket edebilmesi için enerji gerekmektedir,
- Bilgi zaman içinde hareketlenmiş veya durağanlaşmış olabilir,
- Bilginin, katı hali de mevcuttur, donarak katılaşabilir (depolama),
- Bilgi, sıvı hale sahiptir; akar (iletişim yolu ile),
- El sıkışma, baş sallama, bir bakış, bir iç çekiş gibi fiziksel ifadeler bir bilgidir,

- Bilgi birikerek artar,
- Bilgi, verinin belli bir anlam ifade edecek şekilde derlenmiş halidir,
- Bilgi, veri üzerinde yapılan mantığa dayalı dönüşüm, ilişkiler, formüllerin çıktısıdır (Sağıroğlu, 2013: 8).

2.2. Toplumsal Dönüşüm Süreçlerinin Aşamaları ve Bilgi Toplumuna Geçiş

Günümüz bilgi toplumu oluşana dek, insanlık tarihi pek çok aşamalardan geçmiş, değişim ve gelişimler sonucu bugünkü nihai halini almıştır. Günümüz bilgi toplumunun oluşumunu ve gelişimini, temelde iki önemli olayın oluşturduğu söylenebilir. Bunlardan ilki, milattan önce ortaya çıkan ve avcılık ile meşgul olan toplumları, çiftçi ve çoban toplumlarına dönüştürerek, yerleşik hayata geçmelerini sağlayan Tarım Devrimi'dir. İkincisi ise 18. yüzyılda başlayan, buhar makinelerinin önemli rol oynadığı, tarım toplumunu, mal ve hizmet üreticisi sınıfına sokan Sanayi Devrimi'dir (Torun, 2003: 181).

18. yüzyılda buhar makinesinin bulunması ve bunun enerji kaynağı olarak kullanılmasıyla başlayan Sanayi Devrimi süreci, insanlık tarihinin en önemli değişim ve dönüşüm süreci olarak nitelendirilmektedir. Çünkü sanayi devrimi ile birlikte ortaya çıkan yeni teknolojiler, üretim alanlarının farklılaşmasına, bunun sonucunda yaşam biçiminin değişmesine, yeni sosyal yapıların doğmasına yol açmıştır. Hayatını avcı-toplayıcı kültürle idame eden, ilkel toplumlar, sanayi devrimi ile birlikte farklı bir biçimde üretim aşamasının içinde yer almışlardır. Bu dönemde oluşan toplumsal yapı, sanayi toplumu olarak adlandırılmıştır. Bu gelişim ve değişim sürecinde toplumlar, ilkel yaşamdan toprağı işleyerek yerleşik düzenin hakim olduğu tarım toplumuna, tarım toplumundan kitlesel üretimin, tüketimin ve eğitimin önemli olduğu sanayi toplumuna, günümüzde ise sanayi toplumundan kitlesel refahın, bilginin ve nitelikli insan sermayesinin önem kazandığı bilgi toplumuna geçiş şeklinde farklı aşamalardan geçmişlerdir (Aktan ve Tunç, 1998: 118-134).

Bugün ise giderek küreselleşen dünyada, ihtiyaçlar doğrultusunda insanlık tarihini ve buna bağlı olarak şu anki toplum biçimini değiştirecek üçüncü bir devrim ve toplum biçiminden bahsedilmektedir. İşte bu yeni ve köklü değişiminin kaynağı, insanların bilgi anlayışındaki değişim ve teknolojidir. Bunun sonucunda ortaya çıkacak olan

değişimin "Bilgi Devrimi" olacağı bu devrimin de bilgi toplumunu oluşturacağı öngörülmektedir (Torun, 2003: 181). 20. yüzyılın son çeyreğinde bilgi toplumu, sanayi toplumunun yerini almıştır. İlkel toplumdan sanayi toplumuna geçiş ile sanayi toplumundan bilgi toplumuna geçiş süreci kıyaslandığında, sanayi toplumundan bilgi toplumuna geçiş sürecinin daha hızlı gerçekleştiği görülmektedir. Bunun temel nedeni ise, yeni teknolojilerin gelişme hızı ve insanların bu hıza kolayca uyum sağlayabilmesi olmuştur. Günümüzdeki toplum yapısı, sanayileşme sürecine göre teknolojik yeniliklere karşı daha bilgili, bilinçli ve geniş olanaklara sahiptir. Bu da, bilginin en önemli unsur kabul edildiği günümüz bilgi toplumunun, insanlığa getireceği değişim ve dönüşümün, sanayi toplumundan çok daha derin ve köklü olacağını göstermektedir. Sürekli gelişen bilişim ve iletişim teknolojileri sayesinde bilgi, günümüzde her geçen gün daha çok artmakta, bilgiye ulaşım ise her geçen gün gittikçe daha kolay hale gelmektedir. Bilgi odaklı yeni toplum yapısı, hızlı iletişim, sürekli değişim gösteren yeni teknolojiler ile birlikte, bilginin tüm alanlarda temel güç ve kaynak kabul edilmesine yol açmıştır (Erkan, 1997).

Sanayi Devrimine geçişi buhar makinesinin bulunması üstlenmiş ise; bilgi toplumuna geçişi de bilişim teknolojisinin temelindeki araç olan bilgisayarlar üstlenmiştir. Elektronik araçlar ve özellikle bilgisayarlar, bilişim sektörünün temel ürünü kabul edilmektedir. Bilgisayarlar sayesinde, herhangi bir bilginin sistematik olarak saklanması, düzenlenmesi ve gerektiğinde kullanılması ile bilgiye her an ulaşma imkânı doğmaktadır. Bilgi toplumunda, bilgi ve iletişim teknolojisindeki gelişimin oluşturduğu yapı içinde ekonomik faaliyet küreselleşme eğilimine girmiştir. Sanayi toplumunda fabrika üretimi ulusal sınırlardaki pazara yönelikken, bilgi toplumunda bu sınırlar ortadan kalkarak dünya standartları belirleyici konuma gelmiştir. Bilgi toplumunun ekonomik yapısında, sanayi toplumunda ön planda olan maddi mallar yerine bilgi kullanılarak bilginin üretimi ön plana çıkmaktadır. Ayrıca gelişen bilişim teknolojisine bağlı olarak kullanıcıların üretebildiği bilgi miktarı artmakta ve bilgi birikimi olanaklı hale gelmektedir. Bilgi birikiminin oluşturduğu sinerjik etki bilgi üretimi ve bilgiden yararlanmayı da daha hızlı hale getirmektedir.

Günümüz bilgi toplumunun bir uzantısı olan bilişim teknolojileri, insanlara pek çok yarar sağlamakla birlikte, bu teknolojilerin etkili, olumlu ve istenen şekilde kullanılabilmesi için bireylerin yeni beceriler kazanması gerekmektedir. Kurum ve

kuruluşlar, bilgiyi üretebilecek ve kullanabilecek nitelikli insan gücüne ihtiyaç duymaktadır. Bu da bir anlamda kişilerin yetkin kabul edilebilmesi için sürekli gelişen teknolojilere daha iyi adapte olabilmesini, sürekli gelişerek yenilenen bilgi anlayışına uyum sağlamasını gerekli kılmaktadır. Bilgi toplumunun ileri dönemlerinde nitelikli insan ihtiyacı, bilişimsel bilgiye kayarak bu yönde bir ihtiyaç doğuracaktır. Bu da sanayi toplumunun belli bir döneminde yaşanan fabrikalaşma ve bunun sonucunda insan emeğinin ve iş gücünün yok sayılması durumunun bilgi toplumunun ilerleyen dönemlerinde kendini yeniden göstereceği fikrini ortaya çıkarmaktadır.

2.3. Bilgi Toplumu

İnsanlık tarihinin geçirdiği evreleri inceleyen yazarlar bu evreleri; ilkel toplumdan tarım toplumuna, tarım toplumundan sanayi toplumuna ve sanayi toplumundan bilgi toplumuna geçiş şeklinde sıralamaktadır. Bu geçişlerin seyrine bakıldığında; yerleşik tarım düzenine geçişin bin yıl, tarım toplumundan sanayi toplumuna geçişin üçyüz yıl sürdüğü belirtilmektedir. Bilgi toplumuna geçişin ise çok daha kısa bir zaman diliminde gerçekleştiği dile getirilmektedir. Ancak geçiş evresi çok kısa olmakla birlikte bu yeni düzenin insanlık tarihinde çok büyük bir değişime yol açtığı bir gerçektir.

Bilişim toplumu öncesindeki dönemlerde yeni kıtaların, yeni ticaret yollarının, yeni doğal kaynakların keşfedilmesi sonucu ortaya çıkan ekonomik devrimlerden farklı olarak şimdi, bilgisayar teknolojisi ile yaratılan görünmeyen bir sanal dünya keşfedilmiştir (Demir, 2003: 8-9).

Özellikle yirminci yüzyılın sonlarına doğru insanoğlu, tarihinde hiç görmediği kadar hızlı gelişen değişimlere tanıklık etmiştir. Bu değişikliğin, teknoloji ve haberleşmedeki yeniliklerden kaynaklandığı artık bütün dünyanın bilgisi dâhilindedir. Bu yeni durum, ekonomik ve siyasal olarak da farklı bir yapılanma ortaya çıkarmıştır (Güçlü, 2006: 118).

Sanayi toplumunda, o dönemki üretim süreçlerinin, sermaye yapısının ve toplum dinamiklerinin bir sonucu olarak hayata geçmiş olan ulus devlet yapısı, yerini 20.yy.'ın ortalarından itibaren bilgi toplumuna bırakmıştır. Bu değişim ve dönüşüm süreci, sanayi toplumunda gözlemlenen üretim araçlarının, sermaye yapısının ve toplum

dinamiklerinin değişmesine yol açmış, bu durum da toplumun her aşamasında hissedilmeye başlanmıştır.

Bilgi toplumu kavramı, ilk olarak 1962 yılında ABD'li iktisatçı Fritz Machlup tarafından kullanılmıştır (Geray, 2004: 37). Bilgi toplumu kavramını en açık şekliyle tanımlamak gerekirse, bilginin üretim unsurlarından biri haline gelip, ekonomik faaliyetlerin merkezine yerleştiği, ekonomide hem hammadde hem de ürün haline geldiği, herkesin bilgiye eşit olarak eriştiği, bilgi ve iletişim teknolojilerinin yaşamın her alanında giderek artan bir biçimde kullanılmaya başlandığı, insanların yaşama ve iş yapma biçimlerinin değişme uğradığı bir toplumsal yapı olarak tanımlanabilir (Erkan, 1997: 96-101).

Bilgi toplumu; yeni temel teknolojilerin gelişimiyle bilgi sektörünün, bilgi üretiminin, bilgi sermayesinin ve nitelikli insan faktörünün önem kazandığı, eğitimin sürekliliğinin ön plana çıktığı, iletişim teknolojileri, bilgi otoyolları, elektronik ticaret gibi yeni gelişmeler ile toplumu ekonomik, sosyal, kültürel ve siyasal açıdan sanayi toplumunun ötesine taşıyan bir gelişme aşaması olarak tanımlanabilir. 2003 yılı Aralık ayında, Cenevre'de toplanan Dünya Bilgi Toplumu Zirve Toplantısı'nın ilk aşamasında çeşitli ülkeleri temsil eden temsilciler artık herkesin bilgi üretebildiği, bilgiye erişebildiği, mevcut olan bilgiden yararlanarak paylaşabildiği, Birleşmiş Milletler ilke ve amaçlarına dayanan ve İnsan Hakları Evrensel Bildirgesine tamamen saygılı, odağında insan olan, kalkınma amaçlı, Bilgi Toplumu kurma arzularını açıklamışlardır. Aynı toplantıda "Bin Yıl Kalkınma Amaçları" (yoksulluğun ve açlığın ortadan kaldırılması, evrensel eğitimin gerçekleştirilmesi, bebek ve çocuk ölümlerinin azaltılması… gibi) belirlenerek, bu amaçları gerçekleştirmek için bilgi ve iletişim teknolojilerinin kullanılması kararlaştırılmıştır (Tonta ve Küçük, 2005: 8).

2.3.1. Sanayi Toplumu ve Bilgi Toplumu'nun Karşılaştırması

Sanayi toplumu temelde standart mal ve hizmetlerin kitlesel olarak makina ve sanayi kolları sayesinde üretim ve dağıtımına dayanmaktadır. Şirketlerin temel amacı rekabet ortamında üretilen çeşitli mal ve hizmetleri ucuza üreterek daha çok pazar payı elde etmeye yöneliktir. Sanayi toplumunda şirketler "üret-depola-sat" mantığıyla hareket etmektedirler. Kitlesel üretim şekli ve kitlesel dağıtım modeli beraberinde

merkezileşmeyi gerektirir. Örgütsel amaç aynı mal yada hizmeti daha ucuza mal edip, daha hızlı üretmek olduğu için, üretilen mal ve hizmetler sürekli geliştirilmeye çalışılır. Sanayi toplumunda standart mal ve hizmetlerin kitlesel üretimi önemsenmektedir. Çünkü her boya uyan standart mal ve hizmetlerin kitlesel üretimi daha kolaydır. Sanayi toplumunda standart üretime örnek olarak, ABD'de kitlesel olarak üretilen ilk ayakkabılarda sağ ayak – sol ayak ayrımı yapılmadığından, bu ayakkabılara "straights" (düz) adı verilmiştir. Bilgisayar teknolojileri ve bilişim teknolojilerindeki gelişmeler sayesinde, en iyi fiyata, en yüksek kalitede istenilen ürünü üretmek mümkün hale gelmiştir. Sanayi toplumunun üretim mantığı olan, "üret-depola-sat" düzeni, bilgi toplumunda "sat-üret-teslim et" modeline dönüşmüştür. Bilgi toplumunun ekonomik modeli, kişiselleştirmeye dayanmaktadır. Bilgi toplumunda şirketlerin amacı, ürettikleri ürün ve hizmetleri mümkün olduğunca insanların istekleri doğrultusunda kişiselleştirerek, daha fazla müşteri çekmektir. Sanayi toplumundan bilgi toplumuna olan geçişle birlikte artık ülkelerin ihracat ürünleri, tonaj bakımından azalmakta bilgi içeriği yönünden artmaktadır. Tonajın azalmasına karşın, bilgi toplumu ürünlerinin satışından elde edilen gelir katlanarak artmaktadır. Örneğin, nispeten daha az istihdam eden yazılım ve teknoloji şirketleri, büyük demir-çelik ve madencilikle uğraşan şirketlere nazaran daha fazla gelir elde etmektedir. Sanayi toplumunda çalışmak için fabrikaya, eğlenmek için sinemaya, maç izlemek için stadyuma, kitap okumak için kütüphanelere, oyun oynamak için toplu alanlara gidilirken, bilgi toplumunun sağladığı yeni imkanlar sayesinde insanlar artık evinden işlerini takip edip çalışabilmekte, bilgisayar ortamından evinde filim izleyebilmekte, televizyondan maçı, elindeki telefondan veya evindeki bilgisayardan istediği kitabı okuyabilmektedir. Toplumsal düzeni topyekün değiştiren bilgi toplumu dönüşümü halen insanları etkilemeye ve değiştirmeye devam etmektedir. Sanayi toplumunda makine, alet, sistem ve otomasyonun yerini bilgi toplumunda bilgisayar, internet, ağ iletişim ortamı, bilgi ve teknolojik sistemler almıştır. Sanayi toplumu döneminde şirketler açısından taşınamaz mallar ile elde bulunan maddi gereçlere, şirketin sermayesi ve birikimi olarak bakılırken, bilgi toplumunda sermaye algısı olarak fikirlere ve patentlere önem verilmektedir. Sermaye kavramı somutluktan soyutluğa geçmiştir (Tonta ve Küçük, 2005: 3-5).

Bilgi toplumunun temel özelliklerini sanayi toplumunun özellikleri ile karşılaştırmalı olarak şu şekilde sıralayabiliriz;

- Bilgi toplumunun en temel özelliklerinden birisi, sanayi toplumunda ön planda olan "maddi" sermaye yerini, bilgi toplumunda, nitelikli bilgi ve insana bırakmaktadır.
- Klasik sanayi ekonomisinde temel girdi olan hammadde ve toprak gibi geleneksel üretim faktörleri yani doğal kaynaklar yerini bilgi toplumunda, bilgi ve teknolojiye bırakmaktadır.
- Sanayi toplumunda üretilen mal ve hizmetlerin kıtlığı söz konusu iken, bilgi toplumunda bilginin sürekli üretilebilmesi sayesinde bilgi gelişerek artış göstermektedir.
- Sanayi toplumunun üretim ve tüketim faaliyetleri için kullandığı başlıca maddi mallar emek, tabiat, sermaye, girişimci iken, bilgi toplumunda, yoğun teknolojik alt yapı ile birlikte teknik bilgi kullanımı meydana gelmektedir.
- Sanayi toplumunda kas gücünün yerini bilgi toplumunda beyin gücü almaktadır.
- Sanayi toplumunda fabrika üretimi, öncelikle ülkelerin iç pazarlarına hitap ederken, bilgi toplumunda ürün kalite ve standartlarını dünya standartları belirleyici olacak, ürün ve hizmetler küreselleşerek tüm dünyanın hizmetine sunulacaktır.
- Sanayi toplumunda tüketici taleplerinin karşılanmasında mal ve hizmetlerin mobilitesi oldukça düşük, bilgi toplumunda ise bilginin mobilitesi kolaydır. Bu durum, bilginin sınırsız bir tüketici tarafından tüketilmesine ve yenilikleri teşvik etmesine yol açmaktadır.
- Sanayi toplumundaki özel ve kamu iktisadi kuruluşlardan farklı olarak bilgi toplumunda gönüllü kuruluşlar önem kazanmaktadır.

Sonuçta ekonomik yapı, sanayi toplumunun değişim ekonomisinden; bilgi toplumunun sinerjik ekonomisine dönüşmektedir (Aktan ve Tunç, 1998: 118-134).

3. E-DEVLET VE E-DEVLETİ GEREKLİ KILAN NEDENLER

3.1. Devletin Değişen Rolü, Yönetim ve Örgütlenmedeki Değişim İhtiyacı

Toplumsal yaşamın bir zorunluluğu olarak ortaya çıkan devlet kavramı, temel anlamda, vatandaşlarının istek ve gereksinimlerine tatmin edici çözümler bulmak ve hizmet vermekle yükümlüdür. Küreselleşen dünya, hızlı bir değişim sürecinin içinde olduğundan, özellikle bilişim teknolojilerinin hızlı gelişimi, devletlerin toplumlarına ve kurumlarına vermek zorunda oldukları hizmetlerin de değiştirilmesi gerekliliğini ortaya çıkarmıştır. Dünyanın küreselleşerek küçülüp sınırlarının kalkması neticesiyle birlikte, devletler açısından mevcut yönetim politikalarının birçoğu yetersiz kalmış ve yeni bir kamu yönetimi anlayışı ihtiyacı doğmuştur. Söz konusu değişim, toplumların devletten beklentilerinin ve sunulan hizmetlerin kalitesinin artmasına kadar birçok yeni isteği de beraberinde getirmiştir (Çarıkçı, 2010: 100-101).

Bilişim toplumu dönüşüm süreciyle birlikte, toplumda, kamu yönetiminin, eğitim, sağlık, tarım, endüstri, sosyal refah ve güvenlik gibi, vatandaşlarına sunmuş olduğu hizmetlerde yetersiz kaldığı algılamalarının arttığı görülmektedir. Bunun üzerine kamu yönetimleri, gelişen bilgi teknolojilerinin sunmuş olduğu imkanlardan da faydalanarak, bürokratik işlemleri azaltmayı, hizmet sundukları çeşitli alanlarda vatandaşların isteklerini karşılamayı ve kamu masraflarını düşürmeyi hedeflemişlerdir (İç İşleri Bakanlığı, 2004: 10). Kamu hizmetlerinin yurttaşlarının arzu ve beklentilerine uygun hale getirilebilmesi, böylelikle vatandaş-devlet ilişkilerinin düzeltilmesi, vatandaşın kamu hizmetinden yaygın ve zahmetsiz yararlanması, daha şeffaf ve daha demokratik bir devlet-vatandaş ilişkisi e-devlet ve onun getirdiği mobil uygulamalar ile mümkün olabilir (Ülker, 2002: 954).

Günümüzde bireyler ihtiyaçlarını bilgi ve iletişim teknolojileri ile hızlı ve daha ekonomik olarak karşılamakta, bu teknolojilere bağımlı mikro ve makroekonomiler ile yeni iş alanları oluşmakta ve hayat bu teknolojiler doğrultusunda yeniden yapılanmaya başlamaktadır. Bireysel ve toplumsal anlamda veri ve bilgiye erişimin bu denli arttığı ve giderek artacağı yeni teknolojik düzende, devlet de kendisine yer edinmeye başlamıştır. Bu açıdan devletin de işleyiş mekanizmasını gözden geçirmesi ve bu teknolojilerden azami ölçüde faydalanarak, bilgi toplumu bireylerine beklentileri doğrultusunda hizmet

verir nitelik kazanması gerekmektedir. İşte bu değişim ve gelişim gereksinimi, devletin elektronik nitelik kazanmasını, yani E-Devletleşme yolunda adım atmasını mecbur kılmıştır. Gelişen ve değişen toplumun en temel yapı taşı olarak, toplumun bireyleri ve örgütleri rekabet güçlerini arttırmanın yolunun, bilgi ve iletişim teknolojilerini etkin kullanmaktan geçtiğini fark ederek dijitalleşirken, toplumun genel isleyişinden, düzeninden, gelişiminden ve yaşamından sorumlu olan devletin de yapı olarak bu yeni dijital sistemde yer alması ve hatta bu sisteme yeni anlayışlar katarak yol gösterici ve düzenleyici bir rol oynaması bir zorunluluk haline gelmektedir. Bilgi toplumu olma sürecine doğru yol alan ülkelerde, hem gelişen teknolojinin insan hayatındaki kullanılabilirlik alanı, hem de değişen yönetim anlayış tarzının da etkisiyle vatandaşlar devletten çok daha farklı ve çok daha fazla beklenti içine girmişlerdir. Giderek daha karışık hale gelmekte olan devlet-vatandaş ilişkileri, kamu yönetiminde ciddi yapısal değişiklikler yapılmasını zorunlu kılmıştır. Vatandaşların, özellikle hizmet aldıkları birimlerden giderek artan bir oranda açık, şeffaf, maliyet etkin ve verimli çalışmalar talep etmeleri, bilgi ve iletişim teknolojilerinin devletlerin yapısal formlarında da bir araç olarak kullanılmasını gündeme getirmiştir (Gültekin, 2007: 43).

Kamu hizmetlerinin, uygulamada, vatandaşlara nasıl daha etkin, hızlı ve adil bir şekilde ulaştırılabileceği sorusu, öteden beri politik karar vericilerin üzerinde düşündükleri temel konulardan birisidir. Kamu kurum ve kuruluşlarının etkin olup olmadıkları akademik ve politik ortamlarda sıkça sorgulanmaktadır. Teknolojinin kamu yönetiminde kullanılması ve günlük hayata entegre edilmesi anlamı taşıyan E-Devlet aslında bir tür yapılanma süreci olup, kamu yönetiminde yapısal değişimleri gerçekleştirmek, bireysel anlamda ise yönetimi bilişim sistemlerine uyarlamaktır. Devlet ile vatandaş ilişkilerinin elektronik ortama taşınması, E-Devlet kavramının bir aşamasını ifade etmektedir. Burada asıl amaç devlette gerçekleştirilmesi gereken yapısal dönüşümü hayat koşullarına uyarlamaktır. Gelişen bilgi sistem alt yapısı ve bu sistemlerin geniş kabiliyetleri sebebiyle, bireyler vatandaşa karşı daha talepkar olmaktadırlar. Vatandaşların tek düze olmayan talep ve istekleri kamu yönetimlerini esnek olmaya zorlamaktadır. Klasik devlet anlayışındaki "farklı ölçülere aynı beden (one size fits all)" yaklaşımı artık geçerliliğini kaybetmektedir. Büyüyen nüfusa, gelişen ekonomiye ve bireyden bireye değişen kişisel isteklere kamu kurumlarının verebileceği yegane reaksiyon E-Devlet yapılanmasıdır (Baştan ve Gökbunar, 2004: 71-89).

3.2. Küreselleşme Kavramının Yararları ve Sakıncaları

Küreselleşme kavramı yeni bir kavram olmasına, bu güne kadar hakkında çok şey yazılıp söylenmesine karşın, halen devam eden bir süreçtir. Globalleşmenin Türkçe karşılığı olarak kullanılan küreselleşme kavramının en temelinde bilginin küresel düzeyde paylaşımı ve yayılması yatmaktadır. Daha önceleri yerel ve kapalı olan iletişim, finansman, kültür, ticaret, sermaye, spor, popüler kültür, sanayi ve müzik gibi birçok toplumsal faaliyet küreselleşme ile birlikte uluslararası bir niteliğe kavuşmuştur. Ulus-devlet sınırlarını aşan bu etkileşim, değişik ülkelerden insanları bir araya getirmiş, mal, hizmet ve fikir alışverişinde bulunmalarına vesile olmuş, mekânların yakınlaşması, dünyanın küçülmesi, sınırsız ve sonsuz rekabet, serbest dolaşım, pazarın dünya ölçeğinde büyümesi ve ulusal sınırların dışına çıkması gibi yeni kavram ve yöntemleri beraberinde getirmiştir. Küreselleşme, ulusal hükümetlerin ekonomik rollerini azaltmış ve küresel ölçekteki rekabetin ülkelerden çok, uluslararası şirketler arasında yaşanmasına yol açmıştır. Örnek verecek olursak artık küresel rekabet ABD ile İngiltere, Rusya, Japonya, Fransa arasında olmaktan çok Boeing ile Airbus, Samsung ile Apple, HP ile Toshiba arasında olmaktadır (Balay, 2004: 61-63).

İnsan yaşamını temelden değiştiren küreselleşmeyle birlikte, toplum dinamikleri de değişmiş, eski merkezi yönetim sistemleri atıl ve günün değişikliklerine cevap veremez hale getirmiştir. Küresel rekabet, kapitalizmin dünyanın her noktasına erişmesine fırsat vermiş, fakir toplumların gelişmiş ekonomilere karşı gelişeceği varsayımlarının aksine, zengin ile fakir toplumlardaki uçurumu daha da arttırmıştır (Flaten ve Soysa, 2012: 626-629).

Keyman (1999: 71-90)'dan aktaran Yılmaz ve Horzum'a göre küreselleşme:

> Uluslararası ilişkilerde devletin ağırlığının azaldığı, yeni siyasal aktörlerin ortaya çıktığı, sermayenin artık ulusal veya uluslararası değil, küresel bir nitelik taşıdığı, sömürü mekanizmalarının değiştiği, gelişen bilgi sistem teknolojileri sayesinde dünyanın küçük bir köye dönüştüğü yeni bir dünya düzenidir. Küreselleşmeyle birlikte artık dünyanın herhangi bir yerinde meydana gelen bir olay, başka yerlerdeki olayları etkileyebilmekte ve tetikleyebilmektedir (Yılmaz ve Horzum, 2005: 103-121).

Ülke sınırlarının ötesinde rahatlıkla gerçekleşen, serbest ticari faaliyetler ve finansal özgürlük, ulus devletlerarasındaki rekabeti arttırmıştır. Küresel ekonomik bütünleşme, gelişmiş ülkelerde, etkileyici bir ekonomik mobilite sağlamış, firmalar

üzerindeki ulusal otonomiyi azaltmıştır. Süratle çok uluslu yapıya bürünen, eski ulusal firmalar, devlet yönetimlerinin vergi uygulamalarından kurtularak, küreselleşme ile birlikte ulusal vergi gelirlerinin azalmasına sebep olmuşlardır. Küreselleşmenin devlet yönetimine olan etkisi, onu yapı olarak küçültmek şeklinde olmuştur (Meinhard ve Potrafke, 2012: 271-273).

Bilgi toplumunun temel dinamiklerinden olan bilgi ve iletişim teknolojilerindeki ilerleme neticesinde, günümüzde artık uluslararası şirketlerden, ortaklıklardan, küresel yapıdan ve devlet örgütlenmesindeki ciddi değişimlerden bahsedilmektedir. Bu değişim, bilgi ve iletişim teknolojilerinin insan hayatına kattığı sayısız imkân ve faydaların, hantal yapıdaki devlet örgütlenmesini dinamikleştirmede kullanılma arzusu olarak da görülebilinir. Bilgi ve iletişim teknolojilerinin insan hayatında vazgeçilmez bir yere sahip olması ve bu teknolojilerin iktisadi hayatta belirleyici bir yer edinmesi, devletin kendini sorgulaması ve neticesinde de devlet kurumlarının ve örgütsel yapısının tüm işleyiş katmanları ile birlikte yeniden yapılandırılması konularını gündeme getirmiştir.

Küreselleşme, az gelişmiş ülkelere, hızlı büyüme gibi fırsatlar sunmasına rağmen uzun süreçte, gelişmiş ve az gelişmiş ülkeler arasında kutuplaşmaya yol açmaktadır. Küreselleşmenin etkileri sonucu, dünya genelinde, gelir dağılımında dengesizlikler meydana gelmiştir. Küreselleşen pazar ekonomilerindeki bireyler küresel veya yerel şoklara açık hale gelmiştir (Murshed, 2002: 1-3).

Bilgi teknolojilerinin de itici gücüyle, yoğun kültür alış-verişinin yaşandığı sınırları ortadan kalmış küresel bir dünyada, ekonomik bütünleşme politik bütünleşmeyide zorunlu kılmıştır. Yönetimler, sadece tolum ihtiyaçlarını değil küresel ölçekte insanlık ihtiyaçlarını da göz önünde bulundurmak durumunda kalmışlardır. Devlet yönetimlerinin tek başına yetersiz olduğu noktalarda, hükümet dışı organizasyonlar boy göstermiş ve aldıkları çoğu kararla ülkelerin politikilarına etki etmişlerdir (Pudelko vd., 2006: 4-5).

Küreselleşme olgusunun gelişiminde önemli bir yeri olan bilgi ve iletişim teknolojilerindeki yenilikler, kendisini ekonomik ve sosyal yaşamın her alanında göstermekte ve toplumun tüm kesimini çeşitli yönlerden etkisi altına almaktadır (Kumaş ve Birgören, 2010: 29). Her değişim ve dönüşümün olumlu etkileri olduğu gibi olumsuz etkileri de olmaktadır. Küreselleşme kavramının yararları ve sakıncaları şu şekilde özetlenebilir (Balay, 2004: 64-65).

Yararları;

- Küreselleşme ile birlikte zaman ve mekan sınırlamaları ortadan kalkmıştır artık, dünyada meydana gelen her olay bütün insanlığa mal edilmeye başlanmıştır.
- İnsanoğlu küreselleşme süreciyle birlikte bireysel olarak yeni bir kişilik kazanmış, kendine olan güveni ve inancı, evrensel insan hakları, özgürlük anlayışı, adalet ve eşitlik gibi kavramları yeniden tanımlamıştır.
- Toplumda yaşayan kültür ve uygarlık yeni baştan anlamlandırılarak, insanoğlunun ortak değerleri oluşmaya başlamıştır.
- Kitlesel olarak yetişmiş nitelikli bir nüfus yapısına sahip olabilmek için, sadece seçkin bir kesimi eğitmenin yeterli olmadığı, topyekün ülke kalkınması için eğitimin tabana yayılması gerektiği anlaşılmıştır.
- Ülkeler arasında işgücünün serbest dolaşımının sağlanmasıyla birlikte, üretim ve tüketimde rekabet artmış, dünyanın neresinde olursa olsun insanlar birbirlerinin ürünlerinden faydalanmaya ve tüketmeye başlamışlardır.
- İnsanoğlunun hastalıkların önlenmesi ve yayılmasının önüne geçilmesi için sürekli mücadele ettiği sağlık alanında yaşanan uluslararası ortaklık ve akıl birlikteliği sayesinde birçok hastalık yenilmiş veya önemsenmeyecek seviyelere indirilmiş, anne-bebek ve çocuk ölümleri azalmış, insanların yaşam süreleri uzamış, sağlıklı yaşam olanakları genişlemiştir.
- Toplumun tarihsel gelişimi boyunca, devam eden teknolojik gelişmelerin paralelinde, ülke genelinde bireysel hizmet talebi statiklikten dinamikliğe geçmiş ve mobilize olmuştur. Bu yeni talebe cevap verme yarışında olan kurum ve kuruluşlar E-Devlet kavramıyla tanışmış ve hizmet sunumunu mobilize hale getirmişlerdir.
- Sermayenin sınırsız dolaşımı sayesinde, küreselleşme ile birlikte şirketler bazında büyük ortaklıklar ortaya çıkmış, bunun sonucunda da kazanç artışında ciddi farklılıklar yaşanmıştır.

Sakıncaları;

- Küreselleşme sonucunda, güçlü devletlerle bütünleşmek zorunda kalan küçük devletler, ekonomik, siyasal, kültürel ve teknolojik açıdan büyük

devletlerin etkisine maruz kalmışlardır. Bunun sonucunda ise ulusal sınırlar, milli egemenlik ve bağımsızlık gibi kavramlar anlamsızlaştırılarak, emperyalist amaçlar küreselleşme adı altında meşrulaştırılmaya çalışılmıştır.

- Küreselleşme toplumları bir yandan bütünleştirirken diğer yandan ulusalcılık, etnik ulusalcılık ile parçalanma sürecine sokmuştur. Bu nedenle ülkeler, hem küreselleşme sürecinin dışında kalmamak, hem de ulusal bütünlüklerini korumak ikileminde kalmışlardır.
- Ne yazık ki dünyadaki ülkelerin üretim gücü ve refah olanakları aynı değildir. Bu nedenle sanayileşmesini tamamlamış ülkeler daha üstün konumdadır. Küreselleşme sanayileşmesini tamamlamış ülkelere avantaj sağlarken, sanayileşmesini tamamlayamamış veya sanayileşmek üzere olan ülkelerde daha fazla fakirlik ve yoksulluğa neden olmuştur.
- Devletlerin küreselleşme ile birlikte vatandaşlarına verdiği hizmetleri elektronik hale getirmesiyle, E-Devlet kavramı ortaya çıkmış ve siber güvenlik kaygısı yaşanmaya başlanmıştır. Bir anlamda ülke güvenliği artık E-Devlet güvenliği ile paralel hale gelmiştir.
- Küreselleşme ve beraberinde gelişen teknolojik ilerlemelerle dünyada eğitim sürecine katılan insanların sayısı her ne kadar artmakta olsa da, bu eğitim sürecine katılmayan insanların sayısında bir azalma değil, artış olduğu ileri sürülmektedir.

Yukarıdaki örneklerden de anlaşılacağı üzere küreselleşmenin olumlu manada yararlarının yanında olumsuz anlamda sakıncaları da bulunmaktadır. Küreselleşme sürecinin insanlığın gelişimine ve ilerleyişine kattığı en önemli özellik bilgi üretimi, bunun paylaşımı ve öğrenilmesi çerçevesinde olmuştur. Küreselleşme bir yandan yeni iş imkanları ve sahaları yaratırken diğer yandan bu değişimin gerisinde kalmış ülkeleri etkileyerek istihdamı olumsuz yönde etkilemiştir. İnsanlar farklı toplumları ve yaşayış şekillerini keşfettikçe, hayata ve yaşama dair daha fazla bilgi sahibi olmakta, öğrenmiş oldukları yeni bilgiler ışığında kendi toplumlarını ve yaşayış alışkanlıklarını yeniden şekillendirmektedirler. Küreselleşmenin bir sonucu olarak sadece toplum yapıları ve insanların birbirleriyle olan etkileşimleri değişmekle kalmamış, bireylerin devletle veya devletlerin diğer devletlerle olan ilişkileri de değişime uğramıştır. Artık insanlar daha

şeffaf bir yönetim, daha adil bir yaşam düzeni, daha hızlı bir kamu hizmetinin yanında açık bir dünya ve eşit eğitim olanaklarını talep etmektedirler. Bu istekler devletleri bir değişime zorlamakta, bu değişimde bilişim toplumunun isteği doğrultusunda, klasik devlet yönetimi yerine daha fazlasını vaat eden E-Devlet modelinin doğmasını beraberinde getirmektedir. E-Devletleşme sürecine şüphesiz küreselleşmenin etkisi ve katkısı büyüktür (Balay, 2004: 65-66).

3.3. E-Devletin Tanımı ve Temel Bileşenleri

E-Devlet, en temel anlamıyla her ne kadar kamu hizmetlerinin elektronik ortama taşınması faaliyetinin bir sonucu olarak algılansa da, aslında daha derin bir uygulama söz konusudur. Devletin ve uygulamalarının elektronikleşmesinde, bilgi ve iletişim teknolojileri gerçek anlamda birer araç niteliğindedir. E-Devlet, devletin vatandaşlara karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile vatandaşların devlete karşı olan görev ve hizmetlerinin karşılıklı olarak elektronik işlem ve iletişim ortamlarında kesintisiz ve güvenli olarak yürütülmesidir. E-Devletleşme sürecinin temel hedefi ise, bilgi işleme kapasitesi arttırılmış, acil karar alabilen ve ihtiyaçlara hızlı cevap verebilen, mevcut bilgi ve becerisini sistematik bir veri tabanı ile muhafaza edebilen, aynı zamanda bu verilerin güvenliğini çeşitli mekanizmalarla sağlayabilen bir yapının tesis edilmesidir. E-Devlet, vatandaşlara devlet tarafından verilen hizmetlerin, devlet iş süreçlerinin ve uygulamalarının bilgi ve iletişim teknolojileri ile daha hızlı, daha verimli, daha saydam ve daha eşit olarak elektronik ortamda sunulması şeklinde tanımlanabilir (Menteş, 2003).

Bilişim sistemlerindeki teknolojik gelişmelerle birlikte küreselleşmenin de etkisiyle ortaya çıkan E-Devletleşmenin temel amacı, ülke yönetimlerinin küçülmelerine yardımcı olarak maliyetleri azaltmak, devlet-vatandaş ilişkilerini ileri bir aşamaya taşımak, toplumun da isteği olan şeffaf, yoğunlaştırılmış, erişilebilinir ve bürokratik engellerden arınmış bir devlet yönetimini hayata geçirmek olarak sayılabilir. Elektronik sistemleri kullanarak yapılan hizmetin, vatandaş tarafından kullanımı, genelde internet sayfaları aracılığı ile olmakta, E-Devlet uygulamalarıyla bu platform gün geçtikçe cep telefonları gibi mobil platformlara doğru gelişmektedir. Elektronik sistemlerin kesinliği, hızlılığı, kararlılığı her geçen gün bu sistemlerin kullanımını

arttırmakta ve böylelikle kamu yönetiminde yeni bir alan olan E-Devlet terimi gelişerek kendine yer bulmaktadır. Birbirleriyle bütünleşik olarak gelişen ve büyüyen bu sistemler sayesinde, şeffaflık ön plana çıkmakta, böylelikle E-Devlet kavramıyla yolsuzluğun gerilemesine katkı sağlanmaktadır (Hodoş, 2014: 120).

E-Devlet kavramıyla ilgili yapılmış olan tanımların çoğunun ortak noktası devlet işlerinin elektronik ortamda yapılmasıdır. E-Devlet bir uygulama veyahut bir proje değildir. Sürekli takip ve denetim isteyen, sürekli yenilenmesi ve güncellenmesi gereken bir yaşam biçimidir. Sanılanın aksine E-Devlet sanal devlet anlamına gelmemektedir. Gerçek hayattaki devletin, her geçen gün gelişen ve kullanım oranı artan teknolojik olanakları kullanarak, çağın gereklerine uygun hale gelmesi, klasik devlet yapısının teknoloji paralelinde yeniden yapılandırılmasıdır. E-Devlet klasik devlet anlayışının yerine geçecek bir model yönetim şekli değildir. Aksine E-Devlet uygulamaları ve hizmetleri sayesinde, klasik devlet anlayışı içerisinde sunulan ürün ve hizmetlerin daha kaliteli, zamanında ve hızlı ulaşmasıyla mevcut yönetimi sağlamlaştıran ve güçlendiren bir yapıya sahiptir. Devlet tarafından üretilen mal ve hizmetlerin, her aşamasında zaman, enerji ve mali tasarruf sağlaması sebebiyle hem yönetim hem de toplum tarafından tercih edilmesi zorunluluk haline gelmiş olan E-Devlet kavramının uygulanması, günümüz bilişim toplumu dönüşüm sürecinde kaçınılmazdır. Küreselleşmeninde etkisiyle sınırları ortadan kalmış uluslararası pazar, ulusal firmaların hızlı bir şekilde uluslararası forma dünüşmesine yol açmış, bu gelişmelerde vergi veren ulusal firmaların, uluslararası şirket olarak vergilerden kaçmasına sebep olmuştur. Vergi gelirleri azalan ülke yönetimleri, küçülmek durumunda kalmış ve hizmet sunumunda daha ekonomik bir yolun arayışına girmişlerdir (Meinhard ve Potrafke, 2012: 271-273).

Ekonomik gelişmeyle birlikte refah toplumu seviyesinin yakalanmasındaki karmaşık yapılar ve yapısal zorluklar, devlet yönetimlerini yeni arayışalara itmiş, mevcut yönetim modellerini sorgulatmaya başlamıştır. Yönetim performansını vatandaşlara tam anlamıyla yansıtma arayışında olan devlet örgütlenmesi, sürekli büyümek durumunda kalmış, belirli bir aşamadan sonra bu büyüklük yönetilemez bir hal almıştır. Amacı vatandaşlarına hizmet olan devlet örgütü, hantal bir yapıya bürünmüş, başlangıçtaki arzulanan hedeflerinden uzaklaşmıştır. Bu aşamada, bilgi sistemlerinin kullanımıyla, insan faktörünün ortadan kalktığı, önceye nazaran birçok

faydası bulunan E-Devlet modeli, hantal devlet yönetimerine yapısal çözüm sağlamak adına bir umut olmuştur. Yönetim kademesindeki tüm birimlerin varoluş amacının sorgulandığı, yararlı olacakların dönüşüp değiştiği, olmayacakların ise kaldırıldığı E-Devlet sistemi, ülke yönetimlerine, küçük fakat daha etkili bir yönetim yapısı sunmuştur. Vatandaş merkezi hizmet sunumunun hayata geçirilmesi, vatandaş-devlet etkileşiminin maddi anlamda ortaya çıkmasını sağlamış, devlet yönetimlerine olan bağlılık, E-Devletleşme ile daha fazla geliştirilmiştir. Daha önce hesaplanamayan veya hesaplanması oldukça zaman alan fakat neticesinin doğruluğunun kesin olmadığı istatistiksel verilere erişim, E-Devlet uygulamaları ile ölçülebilir olmuştur. Hangi hizmetin ne sıklıkta, hangi dönemlerde ve ne derecede kullanıldığı gibi detaylı istatistikler, devlet yönetimlerine hangi uygulamalara öncelik vermesi gerektiği, hangi uygulamaların çok talep edildiği gibi hizmetin gelişmesine yönelik istatistiki bilgi sunmuştur (Barbosa vd., 2013: 744-745).

E-Devlet, mevcut bilgi işleyiş sürecinin, daha iyi devlet yönetimi oluşturmak için yeniden tasarlanması olarak tanımlanabilir. Köklerini sosyal değişimden alan, yönetimsel değişim ihtiyacıdır. Tüm bireylerin, bu zamana kadar edindiği bilgileri tekrar gözden geçirmesine sebep olan bir süreçtir. E-Devlet teknoloji ile yaratıcılığı harmanlayan bir olgudur. Devlet organizasyonuna, kurum/kuruluşlar ile vatandaşlara teknolojik imkanlarla birlikte yeni bir bakış açısı kazandırmıştır (Bekkers, 2012: 329-334).

E-Devlet uygulamalarının hayata geçebilmesi ve işlevlik kazanabilmesi için, öncelikle tüm devlet kurumlarının, bilgi sistem alt yapılarını oluşturmaları gerekmektedir. Kurumların, bilgi sistem alt yapıları kurulmadan, E-Devlet uygulamalarından söz etmek mümkün değildir. E-Devleti hayata geçirebilme konusunda, iktidarlar, E-Devleti oluşturacak unsurları açısından düzenleyici görev üstlenmeli ve oluşturacakları birimlerin, kurumlar arasında teknoloji ve altyapıdan bağımsız entegrasyonu gerçekleştirmesi gerekmektedir. Devlet, E-Devlet uygulamaları için, öncelikle tüm özel veya kamusal kurumların, bilgi sistem katmanlarının birbirine entegre olabilecek şekilde teşkil edilmesinden, daha sonra denetlenmesinden, güvenliğinden ve özellikle koordinasyonundan sorumlu olmalıdır. Vatandaş, E-Devlet uygulamaları üzerinden, yapacağı işlemleri, devlet kurumlarının oluşturacakları veri tabanlarını kullanan uygulama ve internet siteleri üzerinden gerçekleştirir.

Sitemler arasında uyum ve eş güdüm, ileride oluşacak sorunları önleme adına son derece önemlidir. Devlet, mimari standartlarını belirlemede ve bu süreçlerin koordinasyonunu sağlanmakta yükümlüdür. E-Devlet uygulaması, Devlete, veri toplama ve depolama, kurum içi ve kurumlar arası bilgi paylaşımı, son kullanıcıdan, yönetici seviyesine kadar yetkilendirme, güvenlik, performans, sistem denetimi ve yönetimi, bilgilerin güncellenmesi gibi, sorumluluklar yükler. Kurulacak E-Devlet mimarisine karar verirken, tek denetleyicinin olduğu "merkezi yapı mı?" veya her kurumun kendi bilgi sisteminden sorumlu olduğu "ayrı yapı mı?" oluşturulacağı belirlenmelidir. E-Devlet uygulamasında, şirketlerin, kamu veya özel kuruluşlarının bilgi sistem alt ağ yapılarını gerçekleştirememiş olmaları, E-Devlet sistemi üzerine inşa edilebilecek, e-İmza gibi diğer katmanların uygulanabilirliğini mümkün kılmaz (Baştan ve Gökbunar, 2004: 71-89).

3.4. E-Devleti Gerekli Kılan Nedenler

Geleneksel devlet yapısı, hemen her devlet sisteminde, devletten hizmet bekleyen vatandaşların ve kurumların, sunulan ürün ve hizmetlerin arzu edilen seviyede olmaması gerekçesiyle, verimsiz ve etkisiz olmakla suçlanmıştır. Alınan önlemlere rağmen geleneksel devlet örgütlenmesinde, tarafların tümünün devlet hizmetlerinden aynı düzeyde memnun olduğu bir çözüm oluşturulamamıştır. Bunun sebepleri arasında hizmet talep edenlerin sayıca fazlalığı, sunulan ürün ve hizmetlerin standardize edilmesinin güçlüğü sayılabilir (İto, 2003: 15). Klasik devlet yapısına ve yönetimine etki eden küreselleşme, bilimsel ve teknolojik gelişmeler gibi dış dönüştürücülerin dışında, devletin işleyişindeki hantallık, şeffaf olmayan yönetim anlayışı ve devletin giderek artan harcamaları şeklinde karşımıza çıkan iç dönüştürücüler de E-Devlet oluşumunu hazırlayan faktörler arasında yer almaktadır.

Tablo 1 : Ülkelerin Yıllara Göre İnternet Kullanım Oranları Yüzdesi

Ülke İsmi	2004	2005	2006	2007	2008	2009	2010	2011
Dünya Geneli	14,1	15,8	17,5	20,6	23,2	25,7	29,5	32,8
Avrupa Birliği	46,8	50,9	54,4	60,1	63,9	66,0	69,7	72,1
Almanya	64,7	68,8	72,3	75,4	78,3	79,5	82,5	83,4
Amerika Birleşik Devletleri	65,0	68,3	69,2	75,3	74,2	71,2	74,2	78,2
Belçika	53,5	55,5	59,3	63,9	65,3	69,1	73,7	76,2
Çin Halk Cumhuriyeti	7,3	8,5	10,6	16,0	22,7	29,0	34,4	38,4
Fransa	37,8	41,4	45,2	63,7	68,2	69,1	77,3	76,8
Hollanda	68,3	80,9	83,9	86,1	87,7	89,8	90,7	92,1
İngiltere	65,6	70,0	68,8	75,0	78,2	77,8	77,8	81,7
İran İslam Cumhuriyeti	7,5	8,1	8,8	9,5	10,2	11,1	16,0	21,0
İspanya	44,1	47,9	50,3	54,8	59,1	62,0	65,8	67,9
İtalya	33,3	35,0	38,1	40,9	44,6	48,9	53,7	56,8
Japonya	61,7	66,2	68,0	73,6	74,7	77,4	77,6	78,7
Kanada	65,9	71,6	72,5	73,3	76,7	80,2	80,0	82,7
Lübnan	9,0	10,1	15,0	18,7	22,5	30,1	43,7	52,0
Rusya Federasyonu	12,9	15,3	18,2	24,9	27,1	29,2	43,3	49,3
Türkiye	14,6	15,5	18,2	28,6	34,4	36,4	39,8	42,1
Yunanistan	21,6	24,2	32,5	36,1	38,4	42,6	44,6	53,4

Kaynak : Dünya Bankası, 2013.

Tablo 1 incelendiğinde her geçen yıl dünya genelinde internet kullanım oranı giderek arttığı anlaşılmaktadır. Çoğu ülke sekiz yıl gibi kısa bir sürede internet kullanım oranlarını iki katına çıkarmıştır. Bilgi ve iletişim teknolojilerindeki bu baş döndürücü gelişmeler kendisini başka alanlarda da hissettirmektedir. Özellikle tıp alanındaki gelişmeler sayesinde artık tüp bebek çözümleri ile kısırlığa çare bulunabilmekte, mevcut hastalıklara karşı geliştirilen ve bulunan yeni tedavi şekilleri ile yaşam süreleri uzatılabilmektedir. Bu durum da nüfusun hızla artmasına yol açarak, devletlere her geçen gün eğitim, altyapı, sağlık ve iş taleplerinde ek yük getirmekte, yeni görev ve sorumluluklar yüklemektedir.

İstihdam ve işsizlikle mücadele politikaları sebebiyle devlet kadrolarına alınan ve etkin/maliyet karşılaştırılması yapılmadan vasıfsız işgücünün istihdam edilmesi, devletin hizmet veremez hale gelmesine ve tıkanmasına neden olmaktadır. Bu hantal yapılanmanın doğal bir sonucu olarak devletin verimliliği en alt düzeye düşmektedir. Hantal yapılanmanın getirdiği gereksiz bürokrasiyi azaltarak, iş yapmayan, çalışmayan personeli bünyesinde barındırmayacak bir çözüme gidilmesi kaçınılmaz hale gelmektedir (Gültekin, 2007: 36-39).

Tüm bu faktörler devlet yapısını bilgi ve iletişim teknolojilerinden faydalanmaya ve bu sayede devletin etkinliğini arttırarak, maliyetlerini azaltma arayışına sokmaktadır. Devletlerin, E-Devlet yapılanmalarını, gerçekleştirme nedenleri; devlet işlemlerini şeffaflaştırmak, vatandaşların hayatlarını kolaylaştırılmak ve yaşam kalitesini arttırmak, bürokratik oligarşiyi kırarak işlemlerin, hızlı, etkin ve kesintisiz bir şekilde işlemesini sağlamaktır.

3.4.1. Vatandaş Açısından E-Devleti Gerekli Kılan Nedenler

Devlet hizmetlerinden azami ölçüde faydalanarak, gündelik işlemlerini çözüme ulaştırmak isteyen ülke vatandaşları açısından E-Devlet kavramı incelendiğinde, sayısız faydalarının olduğu görülmektedir. Bunların en önemlilerinin başında, şüphesiz bürokrasiden ve onun getirdiği hantal yapıdan olabildiğince kurtulmak gelmektedir. E-Devlet ve onun getirdiği kolaylıklar sayesinde vatandaşlar, devlet daireleri arasında dolaşmaktan, gerekli gereksiz birçok işlem için uzun sıralar beklemekten ve çok basit küçük uygulamalarla öğrenilebilecek bilgi ve belgelerin ispatı için devlet kurumlarına kadar gitmekten kurtulmaktadırlar. Bütünleşik sistemlerden kurulmuş olan E-Devlet uygulamaları sayesinde, ikametgah yerinden, nüfus bilgilerine, sigorta ve sağlık bilgilerinden adli ve mali bilgilere kadar vatandaşlar hakkında bir çok bilgi, sistemler ve uygulamalar arasında paylaşılmaktadır. Bu sayede işlemlerin hızlanması, doğruluğu ve bütünlüğü sağlanmıştır. Vatandaş olarak her işlem öncesi tekrar yerine getirilmesi gereken basit ama zaman alıcı birçok işlem E-Devlet uygulamaları sayesinde ortadan kalkmaktadır. Her bir vatandaşa verilen özel tanıtım bilgisi sayesinde (TC Kimlik No, Sosyal Sigorta Numarası veya Vatandaşlık Numarası... gibi) hizmet talebinde bulunan vatandaş hakkındaki temel bilgilere çok kısa sürede erişilebilinmektedir.

Hizmet alımı için devlet dairesine giden vatandaşın, muhatap olduğu çoğu kurumu teker teker dolaşması, E-Devlet uygulamalarıyla ortadan kalkmakta bu da vatandaşlara zaman kazandırmaktadır. Basit devlet işlemlerinin yerine getirilmesi, klasik devlet anlayışında gereksiz ulaşım ve kırtasiye harcamalarına sebep olmaktadır. Oysa birbiriyle bütünleşik ve yatay/dikey veri alışverişinde bulunan E-Devlet sistemleri sayesinde vatandaş hem maliyetten hem de zamandan tasarruf eder hale gelmiştir. Günümüzde bilişim toplumu dönüşümü sürecinde, artık katılımcı demokrasinin bir gereği olarak, devlet yönetiminin daha şeffaf ve açık olması talep edilmektedir. Bilinçli tüketici toplumu oluşumu sayesinde, vatandaşlar artık verdikleri vergilerin nerelere nasıl harcandığını bilmek istemektedirler. Kişisel hak ve özgürlüklerin arttığı günümüz sosyal yapısı içerisinde, devlet harcamalarının nerelere yapıldığının gösterilmesi ve paylaşılması, E-Devlet sistemleri sayesinde daha kolay ve anlaşılır şekilde yapılmaya başlamıştır. E-Devlet uygulamalarıyla sağlık, eğitim, güvenlik gibi devletin asli ve zorunlu uygulamalarında oluşturulan bilgi paylaşımları ve ortak veri tabanları sayesinde, vatandaşların bu hizmetlerden yararlanması kolay hale gelmiştir (Türkiye Bilişim Derneği, 2013).

3.4.2. Şirketler Açısından E-Devleti Gerekli Kılan Nedenler

E-Devlet uygulamalarının şirketlere getirdiği faydalar incelendiğinde, en önemli faydalarının başında, tüzel kişiliğe sahip firma ve kurumların yine gerçek kişilerde olduğu gibi, klasik devlet bürokrasinden ve onun getirdiği hantal işleyiş mekanizmasından kurtulabilmesidir.

Geleneksel devlet anlayışında iş kurma veya yeni şirket oluşumu süreçlerinde istenen belge ve bilgiler girişimcileri zorlamaktadır. Bürokrasinin getirdiği bu hantal yapının işleyişi zaman almakta ve günümüz küresel rekabet şartlarına uymamaktadır. E-Devlet sistemleri sayesinde tüzel kişiliklere sahip olan kurum ve şirket evrakları hızlı bir değerlendirme sürecinden geçirilerek e-ticaretin önü açılmakta ve girişimci vatandaşların ekonomiye daha hızlı kazandırılmalarını sağlamaktadır.

Geleneksel yapıda zaman alan, ihracat ve ithalat işlemleri, E-Devlet uygulamaları sayesinde hızlandırılmakta, istenilen izinlerin veya onayların hızlı alınabilmesi sağlanmakta ve böylelikle iş dünyasının rekabet şansı etkilenmemektedir. Kalite

standartlarındaki değişim veya devletin üretim için sunduğu teşviklerin içeriklerinin internet veya E-Devlet uygulamaları üzerinden duyurulması sayesinde üretim bandında oluşabilecek yanlış veya kusurlu ürünlerin önüne geçilerek, ürün planlanmasında kayıp yaşanması önlenebilmektedir (Türkiye Bilişim Derneği, 2013).

3.4.3. Kurumlar Açısından E-Devleti Gerekli Kılan Nedenler

Yatay ve dikey yönetim örgütlenmesi içerisinde görevini sürdüren, gerek kamu kurum ve kuruluşları, gerekse özel sektör kurumları olsun, tüm kurumlar, bilginin anlamlı bir şekilde planlanıp, tasnif edilmesine ihtiyaç duyarlar. Elde bulunan bilginin güncelliğini sağlayamama sonunda oluşan bilgi kirliliği, kurumların işleyişini önemli ölçüde etkilemektedir. Kamu kurumlarını birbirine bağlayan iletişim ağ alt yapısının olmaması, kurumların birbirinden bağımsız ve mükerrer kayıtlar tutmasına sebep olmakta bu nedenle hizmet amaçlı her faaliyette kaybedilen zaman, enerji ve para ciddi boyutlara ulaşmaktadır.

Birçok kurumda, yürütülen hizmetlerin kayıtlarının tutulması ve hizmet arşivinin sağlanması amacıyla, aynı özelliğe sahip verilerin ayrı ayrı saklanması sebebiyle yapılan israf büyük boyutlara ulaşmaktadır. Ortak veri tabanı olmadığından her kurumda ayrı ayrı tutulan bu veriler, zaman kaybına sebep olmaktadır. Kurumlar arası iletişimde ve koordinasyonda, kullanılabilecek veriler sağlıklı olmadığından hizmet kollarında gerçeği görememe gibi yönetimsel sorunlar meydana gelebilmektedir. E-Devlet sürecinde, devlet önderliğinde belirlenen mimari yapı çerçevesinde haberleşen ve yetkilendirilen sistemler sayesinde, bilginin güncel olması, tek elden yönetimi ve doğruluğunun sağlanması kalaylıkla yapılabilmektedir. Ortak veri tabanını kullanan bütünleşik bir E-Devlet sisteminde, mükerrer kayıtların önüne geçilebilmekte, kurumlar için ileriye dönük hizmet kollarının faydalanabileceği istatistiki verinin kolay, hızlı ve gerçekçi bir şekilde elde edilebilmesi sağlanabilmektedir (Türkiye Bilişim Derneği, 2013).

Tablo 2: Bireylerin, Kamu Kurumlarıyla İletişimde İnterneti Kullanma Oranı (%)

Açıklama	Türkiye	Kent	Kır
Kişisel amaçla kamu kurum / kuruluşlarıyla iletişimde İnterneti kullananların oranı	45,1	47,5	32,9
Yürütülen faaliyetler			
Kamu kuruluşlarına ait web sitelerinden bilgi edinme	42,9	45,3	30,8
Resmi formları / dokümanları indirme	15,7	16,6	11,1
Form doldurma veya doldurulmuş form gönderme	17,3	18,4	11,9

Kaynak: DPT, 2011.

Tablo 2'de Türkiye'de Nisan 2011 – Mart 2012 ayları arasında internet kullanan bireylerin kişisel amaçla kamu kurum/kuruluşlarıyla iletişimde interneti kullanma oranları gösterilmiştir. İnterneti kullanan bireylerin %45,1'i kamu kurum ve kuruluşları ile iletişimde, interneti tercih etmektedir. Bu bireylerin kullanım amaçları incelendiğinde, bilgi edinme, form/doküman indirme veya doldurulmuş formları/dokümanları gönderme amacıyla kamu kurum ve kuruluşlarının internet sitelerini ziyaret ettikleri anlaşılmıştır. 2012 yılı itibariyle interneti kullanan bireylerin %45'inin kamu kurum ve kuruluşlarıyla iletişimde İnternet'i kullanıyor olması, kurumlar açısından elektronik iletişimin toplum nazarındaki önemini göstermektedir. Gelişen ve değişen toplum isteklerine cevap verebilmek için kurumlar da E-Devlet sistemlerine uyumlu olarak dönüşmeli ve değişmelidir.

3.5. E-Devletin Temel Amaçları ve Sağlayacağı Faydalar

Vatandaşların, özel kurum ve kuruluşların, hatta birbirinden ayrı yapıda teşkil edilmiş devlet yapılarının kendi aralarındaki iletişimlerini internet üzerinden gerçekleştirmesi zaman ve mekan anlamında büyük avantaj sağlarken, ülke ekonomisi de bu durumdan kazanç elde etmektedir. Elektronik işlemlerin sağladığı erişilebilinir hizmet sunumu sayesinde, artık saat sınırı ortadan kalkmakta, bürokratik işlemler en aza inerek evrak getir-götür süreçleri bertaraf edilmekte ve en önemlisi de yapılan her

işlemin saati, dakikası ve içeriği kaydedilerek, rüşvet ve yolsuzlukların önüne geçilmektedir. E-Devlet uygulamalarının devlet yönetimine kattığı şeffaflık yeteneği sayesinde, her bir birey ve kurum devlete eşit mesafede yer almakta ve böylelikle devlet hizmetlerini görebilme açısından vatandaşlara fırsat eşitliği sağlanabilmektedir.

Daha önce belirtildiği üzere, klasik devlet kurumları kendilerinden beklenen hizmetleri karşılayamamaktadır. Yaptıkları kırtasiye ve bürokrasiye dayalı olan hizmetler, harcamaların artmasına ve işlemlerin çok zaman almasına sebep olmaktadır. Günümüz bilgi toplumunda bireyler, kendilerine hizmet veren kurumların daha hızlı, daha doğru ve daha az maliyetle hizmet vermelerini beklemektedirler. Bu yeni devlet anlayışı, kamu kurumları ile bireylerin ilişkilerini, daha şeffaf ve hızlı bir işleyişe sevk etmektedir.

> E-Devlet ile devlet-vatandaş ilişkileri karşılıklı olarak bilgi sistem ağ yapısı sayesinde zaman ve mekân ayrımı olmaksızın sunulabilmekte, vatandaşlar ise bazı görev ve sorumluluklarını bu bilgi sistem ağı üzerinden yerine getirebilmektedirler. Bu bakımdan, E-Devleti sadece teknolojik olanakların kullanımı olarak algılamak, E-Devleti eksik yorumlamak ve düşünmek anlamına gelmektedir. E-Devlette vatandaşlar ürün veya hizmet zincirinin basit bir halkası olmamakla beraber, yönetim sürecinin aktif bir katılımcısı haline gelmektedir (Balcı vd., 2003: 267'den aktaran Çarıkçı, 2010: 100-101).

E-Devlet uygulamalarının kamusal hizmetlerde kullanımında elde edilecek faydalardan bazılarını şu şekilde sıralayabiliriz;

- Vatandaşlar ve hizmet alıcılar tarafından, kamu hizmetine erişimde, en büyük engeller arasında gösterilen bürokrasinin, E-Devlet uygulamaları sayesinde azaltılmasının sağlanması, ihtiyaçlara ve isteklere hızlı ve güvenilir erişimin sağlanması,
- Devletin E-Devlet uygulamaları sayesinde hızlı ve etkin bir şekilde işleyişinin sağlanması ve bu sayede sunulan hizmet kalitesinin artırılması,
- Devlet vatandaşlarının, kamu kurum ve kuruluşlarına gitmek zorunda kalmadan, her yerde ve her zaman devletten hizmet alabilmesiyle, kolay, hızlı ve rahat erişimin sağlanması,
- Devlet-birey etkileşiminin ve dikey iletişimin sağlanması ile bireyle devlet arasındaki bağın kuvvetlenmesi, vatandaşın yönetime etkin katılımı,

- E-Devlet uygulamaları ile sağlanan kırtasiye, kağıt, personel, alan ve makam tasarrufu sayesinde, mali tasarruf sağlanması ve ekonomik gelişimin desteklenmesi,
- Kamusal hizmetlerin erişiminin kolay olması sebebiyle, uygulamalara ve uygulamalar üzerinden hizmete erişimin kentsel alanlardan ülkenin en ücra noktalarına kadar yaygınlaştırılması,
- İnsan faktöründen kaynaklanan hata unsurlarının, bilgisayar sistemleri sayesinde en aza indirilerek, kamu hizmetlerindeki hata oranının azaltılması,
- Kamu kuruluşlarının çalışmalarında ve denetiminde bilgisayar teknolojisinin kullanılması sayesinde, hizmet ve iş verimliliğinin artması,
- Vatandaşların, saat ve gün sınırlaması olmaksızın, kamusal hizmetlere, bilgi sistemleri üzerinden erişim sağlamasıyla, kamu yönetiminde kesintisiz hizmetin sunulması,
- Mevcut belge ve bilgilerin, elektronik sistemlere aktarılmasıyla işlemlerin kayıt altına alınması, eski evrak ve kayıt ortamına oranla şeffaflık ve hesap verilebilirliğin artması, bu sayede güven ortamının sağlanması,
- Denetim faaliyetlerinin elektronik sistemler üzerinden yapılması sayesinde uzun zaman alan tasnif ve tasfiye işlemlerinin, hızlı ve ekonomik olması, bu sayede önlem ve tedbirlerin zamanında alınabilmesinin sağlanması (Saraçbaşı, 2010: 33-36).

Yukarıda bahsedilen maddelerin E-Devlet süreci içerisinde gerçekleşmesiyle; zamandan kazanç, maliyetlerin düşmesi, verimliliğin artırılması, memnuniyetin artırılması, ekonomik gelişimin desteklenmesi, hayat kalitesinin artması, bireysel katılımın artması gibi yararlar sağlanacaktır.

3.6. Geleneksel Devlet / E-Devlet Karşılaştırılması

Geleneksel devletin hizmet ve vazifelerini yerine getirebilmesi için gerekli olan tüm temel unsurlar, esas itibariyle E-Devlet için de geçerlidir. Lakin bilgi çağının kendine has yapısı sebebiyle, bu unsurların tamamı geleneksel yapıdan farklı bir içerik ve boyuta dönüşmektedir. E-Devlet uygulamaları, ağ üzerinde yapılandırıldığından E-

Devleti oluşturan unsurlar da bilişim sistemleri üzerinde çalışmaktadır. Böylelikle devletin her unsuru birbirine elektronik olarak bağlı çalışmakta ve devletin kurum ve kuruluşlarla arasında eşgüdüm daha rahat sağlanmaktadır. Farklı kurumlarda yapılan aynı işlemin tekrarı ortadan kalkmakta, vatandaş-devlet ilişkilerinde büyük ölçüde zaman ve maliyet tasarrufu sağlanmakta ve hizmetler etkin bir şekilde yerine getirilmektedir. Geleneksel devlet sistemlerinde her şey yasalar ve kurallarla belirlenmiştir. Toplumsal düzenin temelini ve kurallarını belirleyen bu yasalar, toplumsal ihtiyaçlarda meydana gelen değişikliklerle birlikte düzenlenmekte ve bu değişim ihtiyaçları karşılanmaya çalışılmaktadır. Ancak geleneksel toplum yapıları çok yavaş değişmektedir. Buna rağmen bilgi toplumunda her şey çok hızlı bir şekilde değişmekte ve toplumsal ihtiyaçlar günden güne farklılaşmaktadır. Değişimin hızı, dinamiği ve canlılığı toplumdaki tüm sosyal ve ekonomik işleyişleri yeniden yapılandırmakta ve "vatandaş-devlet" ilişkilerinde şimdiye kadar hiç olmadık şekilde karşılıklı etkileşim, iletişim yaşanmaktadır. Kurumlar ve bireyler farklı uygulamaları kolaylıkla görüp karşılaştırabilmekte ve talep edebilmektedir (Saraçbaşı, 2010: 33-36).

Geleneksel devlet anlayışında devlet örgütlenmesi genelde tek yönlü olarak düzenlenmekte ve yukarıdan aşağıya bir hiyerarşik yapı şeklinde tezahür etmektedir. Bu yapıda, vatandaşların yönetime ve yönetim süreçlerine katılımı ile ortaya çıkan bilginin paylaşımında sorunlar yaşanmaktadır. Fakat ağ ortamında iletişim iki yönlü olduğundan hemen her konuda vatandaş ile veya kurumlar ile işbirliği tesis etmek son derece kolay olmaktadır. Bu etkileşim ortamı sayesinde kamu hizmetlerinin sürekli iyileştirilmesi, geliştirilmesi ve vatandaş memnuniyetinin sağlanması geleneksel devlet örgütlenmesine göre daha hızlı ve kolay bir biçimde gerçekleştirilebilmektedir. Geleneksel devlet örgütlenmesinin merkezi ve birbirinden kopuk birimlerden oluşan yapısı yerine, elektronik devlette birbiriyle bağlı, bilgiyi paylaşan, vatandaşlarının talep ettiği çeşitli hizmetleri zaman ve mekân farkı gözetmeksizin sürekli olarak sağlamaya yönelik bir örgütlenme yapısı söz konusu olmaktadır. Bu dönüşümün başlangıcı, bütün vatandaşları ortak bir veri tabanında toplayacak uygulamaların hizmete sunulmasıdır. Vatandaş kimlik numarası, sicil numarası ve benzeri uygulamalarla her bir vatandaşı bir profil olarak tanımlayan ve gören ağ teknolojisi uygulamalarıyla, sunulan farklı hizmetlere ulaşabilmektedir. Bilişim teknolojilerinin etkin kullanımı sayesinde, ağ teknolojileri ve ağ mantığına göre yapılandırılan devlet örgütlenmesinde, kişiler, kurumlar, şirketler ve

devletlerarası ilişkiler farklı bir konumda olmaktadır. Genel itibariyle E-Devlet uygulamalarını başlatan birçok ülkenin E-Devlet uygulamaları, ağırlıklı olarak geleneksel devlet yapısında yaşanan yönetim sorunlarını aşabilmek amacını taşımaktadır. E-Devletle birlikte daha etkin ve verimli bir devlet yapısı oluşturmak, hizmet maliyetlerini düşürmek, daha fazla sayıda vatandaş ya da kuruma aynı anda mekân ve zaman fark etmeksizin hizmet verebilmek, verilen hizmetlerin kalitesini arttırmak mümkün hale gelmektedir. Ancak bu tarz bir yönetim anlayışının sağladığı sayısız yararların yanında bazı sakıncalar da vardır. Sistemin ne derece korunaklı olduğu, olası savaş ve gerginlik durumlarında nasıl çalışacağı, teknolojinin hızla gelişmesi sebebiyle yeni kurulan veya alınan bir sistemin etkin kullanımından önce atıl hale gelmesi, vatandaşların gelişen teknolojiyi izlemekte zorlanmaları ve elektronik devletle iletişimde sıkıntılar yaşamaları, devlet yapısının ve dolaylı olarak diğer kamu veya özel kuruluşlar ile vatandaşların, ağ sistemine dahil olabilmeleri için yapmaları gereken alt yapı ve asgari teknolojik harcamalar bu sistemin zayıf yanları olarak adlandırılabilinir (İto, 2003: 17-39).

E-Devlet sayesinde, mekan ve maliyet unsurlarını kendi lehine çeviren devlet vatandaşları üzerindeki etkinliğini arttırmaktadır. Daha fazla sayıda vatandaşa, eş zamanlı olarak aynı kalitede hizmet verebilmek, ancak E-Devletleşme sayesinde mümkündür. E-Devlet her ne kadar teknolojik yatırım için kaynak harcanmasını zorunlu kılsa da uzun vadede vatandaşa sunulan hizmetin maliyetini büyük ölçüde düşürerek, geleneksel devlet örgütlenmesinin yaşadığı kaynak sorununun çözümüne yardımcı olmaktadır. Geleneksel Devlet yapılarında ekonomik faaliyetler gibi yakinen ve anlık takip edilmesi gereken, sürekli değişen ve akan bilginin izlenmesi, denetlenmesi ve kayıt altına alınması sağlıklı bir şekilde yapılamamakta, ekonomik değerler üzerinden vergi tahakkuk ve tahsilatı yapmak gibi işlemler çok fazla kırtasiye ve bürokrasiye neden olmaktadır. Ağ sistemleri ise bu tarz sorunları büyük ölçüde ortadan kaldırmaktadır (Saraçbaşı, 2010: 33-36).

E-Devlet uygulaması, klasik devlet anlayışındaki çoğu aksaklığın önüne geçerken, aynı zamanda birçok yeniliğin vatandaşa sunulması ve devlet işlerinde kullanılmasını sağlamıştır. Tablo 3'de, geleneksel devlet yapılanması ile E-Devlet uygulamalarının karşılaştırılması verilmiştir. Kamusal alanda karşılaşılan olumsuz faktörlerin, E-Devlet uygulamaları ile gündemden kalktığı görülmektedir (Uçkan, 2003).

Tablo 3: Geleneksel Devlet ve E-Devlet Karşılaştırması

Geleneksel Devlet	E-Devlet
Pasif Yurttaş	Aktif Müşteri-Yurttaş
Kağıt-temelli İletişim	Elektronik İletişim
Dikey/Hiyerarşik Yapılanma	Yatay/Koordineli Ağ Yapılanması
Yönetimin Veri Yüklemesi	Yurttaşın Veri Yüklemesi
Eleman Yanıtı	Otomatik Sesli Posta, Çağrı Merkezi vb.
Eleman Yardımı	Kendi kendine Yardım / Uzman Yardımı
Eleman-temelli Denetim Mekanizması	Otomatik Veri Güncellemesiyle Denetim
Nakit Akışı / Çek	Elektronik Fon Transferi (EFT)
Tektip Hizmet	Kişiselleştirilmiş/Farklılaştırılmış Hizmet
Bölümlenmiş / Kesintili Hizmet	Bütünsel / Sürekli / Tek-duraklı Hizmet
Yüksek İşlem Maliyetleri	Düşük İşlem Maliyetleri
Verimsiz Büyüme	Verimlilik Yönetimi
Tek Yönlü İletişim	Etkileşim
Uyruk İlişkisi	Katılım İlişkisi
Kapalı Devlet	Açık Devlet

Kaynak: Uçkan, 2003.

4. BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK KAVRAMI

4.1. Bilgi Güvenliği Tanımı, Kavramları

Bireyler için özel bilgilerin, kurumlar için teknik veya kurum içi bilgilerin gizliliğinin sağlanması esas olduğu gibi devletler için de kamusal bilginin gizliliği ve bütünlüğü önem arz etmektedir. Fiziki ortamda tutulan hemen hemen tüm veri ve dokümanlar E-Devletleşme süreci ile birlikte bilgisayar ortamına aktarılmakta ve bu verilerin güvenliği, gelişen ve değişen teknoloji nedeniyle her geçen gün daha kırılgan

hale gelmektedir. Bilgi güvenliği, kurumların bilgi envanterindeki varlıkların gizliliğini, bütünlüğünü, erişilebilirliğini, hesap verilebilirliğini ve yetkilendirilmesini sistematik bir güvenlik politikasıyla belirlemesi ve olası ihlallerde inkâr edilemeyecek şekilde koruma altına alma yönetimidir.

Bilgi güvenliği kurumun veya devletin dünya çapında rekabetçi gücünün korunması, para akışının sürekliliğinin sağlanması, karlılığın artırılması, piyasa işlevselliğinin korunması, yasal uyumluluğun sağlanması ve kurumsal imajın zedelenmemesi için gereklidir. Bilgi sistemleri temelde güvenlik amacıyla değil, işlevsellik amacıyla tasarlanmıştır. Kurum ve devlet hizmetlerinin, E-Devlet uygulamaları ile birlikte, giderek bu güvensiz ortamda yürüyor olması güvenliğe olan ihtiyacı artırmaktadır.

Özellikle 21.yüzyılın başlarından itibaren meydana gelen olay ve yaşanan olgulardan sonra, bilgi güvenliği dünya gündeminde olan bir konudur. Genel olarak bilgi güvenliği, "bilgi değeri taşıyan verilere, izinsiz erişimin engellenmesi, ifşa ve kötüye kullanmanın önüne geçilmesi, değiştirilmesi, zarar ve kayıptan koruması amacıyla kullanılan işlem ve teknolojilerin toplamıdır." (Unctad, 2005:187) şeklinde tanımlanabilir.

Bilgi güvenliği kişi ve kurumların "Bilgi Teknolojilerini" kullanırken karşılaşabilecekleri tehdit ve tehlikelerin daha önceden gerekli analizlerini yaparak, alınması gereken önlemlerin alınmasını sağlamak olarak tanımlanabilmektedir. Bilgi güvenliğinin amacı, doğru teknolojinin, doğru amaçla ve şekilde kullanılmasını sağlayarak, bilginin her türlü ortamda istenmeyen kişiler veya sistemler tarafından ele geçirilmesini önlemektir (Sağıroğlu, 2013: 14). Bilgi güvenliği konusunu daha anlaşılabilir olması için, altı kavramın incelenmesi gerekmektedir. Bu kavramları; Gizlilik, Bütünlük, Erişilebilirlik, Hesap verebilirlik, Yetkilendirme, İnkâr edememe başlıklarında inceleyecek olursak;

4.1.1. Gizlilik

En temel tanımı ile gizlilik kavramı; kuruma veya bireye özel bilgiye, sadece yetkilendirilmiş kişilerce ulaşılabilmesidir. Gizli bilgi avukat-müvekkil veya doktor-hasta ilişkisi gibi bireysel anlamda olabileceği gibi, bir ürünün üretim aşaması gibi

kurum ve kuruluşlar için teknik bir bilgi de olabilmektedir. Bilginin gizliliğinin muhafazası, bilginin değerine göre önem taşımaktadır.

4.1.2. Bütünlük

Bütünlük (veri/bilgi bütünlüğü) verinin veya bilginin yetkisiz kişilerce değiştirilmesine veya yok edilmesine karşı korunmasıdır (www.cnss.gov, 15.08.2012). Verinin bozulması, kasten veya istemeyerek olabilir. Verinin arzu edilen bütünlüğünün korunması için yetkisiz değişim veya bozulmalara karşı korunması gerekmektedir.

4.1.3. Erişilebilirlik

Doğru yetkilendirilmiş bir kişinin ihtiyacı olduğu anda ihtiyacı olan hizmetin veya servisin kullanılabilir/erişilebilir olma durumuna erişilebilirlik denir. Verilen hizmetin ne kadar güvenilir olduğunun ölçütüdür. Kurumlar sundukları hizmetin önemine göre sistemlerini ve verilerini yedekli hale getirirler (www.cnss.gov, 15.08.2012). Bir başka tanımla erişilebilirlik; Kurumsal bilgi ve kaynakların ihtiyaç duyan kişilerce sürekli erişilebilir durumda olması kavramıdır.

4.1.4. Hesap Verebilirlik

Hesap verebilirlik kişisel sorumluluğun bir ölçütüdür. Hesap verebilirliğin en kısa tanımı, kişilerin yaptıkları ve görevi olduğu halde yapmadıklarından sorumlu olmalarıdır (www.cnss.gov, 15.08.2012). Kamu kurumlarında hesap verebilirliğin en önemli yansıması şeffaflıktır. Şeffaflık devlet örgütlenmesinde, kamu kaynaklarını kullanmakla görevli yetkililerin, eylemlerini, icraatlarını ve planlarını anlaşılabilir bir halde, olduğu gibi, değiştirmeden kamuoyu denetimine açmalarıyla uygulanabilir.

4.1.5. Yetkilendirme

Bilgi güvenliği bağlamında yetkilendirme, kimlik doğrulama sistemidir. Bilgiye erişim sürecinde yetkilendirme, bilgiye doğru yetkili kişi veya sistemin erişip erişmediğini kontrol eden alt sistemdir. Kullanıcı bazında yetkilendirme olabileceği gibi, uygulama bazında da yetkilendirme olabilir. Yetkilendirme mekanizması ile bilgiye erişimin sınırlandırılması sağlandığı gibi bilginin anlamlı bir bütün halinde muhafaza edilmesi de sağlanmış olur. Uygulamaları sadece okuyacak, ekleme yapacak, güncelleme yapacak, sistem üzerinden kaldıracak personele veya uygulamalara verilecek yetkiler verilirken dikkat edilmeli, gereksiz yere yetki verilmesinin önüne geçilmelidir.

4.1.6. İnkâr Edememe

Bilgiye ve veriye kimin, ne zaman, nasıl, nereden, ne şekilde eriştiğinin takibinin yapılabilmesi ve erişen kişinin kimliğinin açıkça belirtilmesi sürecidir. Kullanıcı adı, parola, manyetik kart gibi tanıtma ve tanımlama sistemleri kullanılabildiği gibi biometrik (retina, parmak izi, avuç izi... gibi) teknolojilerle de erişim ve inkar edememe kontrolü sağlanmaktadır.

4.2. Bilgi Güvenliği Yöntemleri ve Tedbirleri

Kurum ve kuruluşların sahip olduğu bilginin; gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından sürekli korunması gereklidir. Bir kurum, en ileri güvenlik teknolojilerini, en gelişmiş ve pahalı sayılabilecek teknolojik sistemleri kendi yapısına uygulasa dahi o kurumda bilgi güvenliğinin tamamen sağlandığından asla bahsedemeyiz. Günümüzde saldırganlar, siber saldırılarda, artan güvenlik teknolojileri dolayısıyla kurum ve kuruluşlardaki teknik açıkları kullanma veya onlardan faydalanma yolundan ziyade, nispeten daha kolay olan, insan unsurunun zayıflıklarından faydalanma yoluna yönelmişlerdir. Bundan dolayı kurum ve kuruluşlarda güvenliğin en zayıf halkasını hala insan unsuru oluşturmaktadır. Güvenlik kavramı; teknolojiden daha

önce insana yatırım yapılmasıyla, kurum çalışanların en tepeden en alt çalışanına kadar, gerekirse müşteri ve ziyaretçilerini de bilgilendirerek, onlar üzerinde bir bilgi güvenlik farkındalığı oluşturması ve desteklemesi ile anlamlı hale gelebilir. Her türlü teknolojik donanımla donanmış olsa dahi, herhangi bir bilgi sistemini en nihayetinde kullanacak insan faktörünün eğitilmesi ve bilinçlendirilmesi bilgi güvenliğinde onun yol açacağı bilinçli/bilinçsiz güvenlik risklerini hiçbir zaman tamamen ortadan kaldırmasa da, iyi planlanmış bir farkındalık faaliyeti ile güvenlik risklerinin kabul edilebilir bir seviyeye çekilmesini sağlanabilir. Bilgi güvenliği risklerinden korunmanın en iyi yolu, bilgi teknolojilerine ve alt yapısına çok para harcamaktan önce, sistemi kullanan veya hizmetten faydalanan insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojisinin doğru yer ve zamanda kullanılmasıyla mümkün olabilir (Şahinaslan vd., 2009: 597-600).

İstenilen bilginin kurumlar arasında güvenli bir şekilde iletilmesi ve paylaşılması, işlemlerin elektronik ortamda güvenle yapılabilmesi ve yaygınlaşabilmesi açısından önem taşımaktadır. Kurumların bilgi sistemleri, güvenli olmayan internet ortamına bağlı olması sebebiyle, güvenlik risklerine karşı koruma sağlayacak şekilde tasarlanmalı ve yapılandırılmalıdır. Bu sayede vatandaşlar, kamu kurumları ve iş çevreleri arasında güvenli bir etkileşim sağlanmış olacaktır (Başbakanlık, 2005/20: s:13). Bilgi güvenliğinde, bilginin korunması üretim aşamasından başlayarak erişim, işleme, depolama, aktarma ve yok etme aşamalarına kadar sağlanmalıdır.

4.2.1. Elektronik İmza

E-Devlet uygulamalarının işlerliğini sağlayan en önemli unsur temelde e-belge yönetimidir. E-Devlete geçiş sürecinde e-belgeler yada e-evraklar üzerinde önemle durulması gerekmektedir. E-Devlet süreciyle beraber, devlet hizmetlerinin elektronik ortamdan yürütülmeye başlamasıyla birlikte, hukuki davalara kanıt sağlama, ülke adına önemli kararları verme, personel kişi veya kurumlar hakkında tasarrufta bulunma, kurum ve kuruluşlar arası önemli, gizli bilgi alış-verişinde bulunma, ulusal kalkınma ve gelişmenin izlenmesi gibi birçok önemli işlem, e-belgeler üzerinden gerçekleştirilmektedir. E-Devletin temel amaçları arasında bulunan bürokrasinin azalması amacıyla kamu kurum ve kuruluşlarının ürettiği bilgi ve belgeler kamu

erişimine açılmaktadır. Elektronik ortama alınan bu belge ve verilerin doğruluğunun sağlanabilmesi ve aynı zamanda kağıt ortamından dijital ortama aktarılmış verilerin dolaşımının kontrollü bir biçimde sağlanabilmesi için yine bu bilgi ve belgelerin elektronik olarak imzalanması gerekmektedir. Elektronik imza dijital bilgi ve belgelerin yasal geçerlilik kazanmasında önemli bir yere sahiptir. E-ortamda hizmet verilmeye başlandığında kamu kurum ve kuruluşlarınca veya özek kuruluşlarca verilecek kararlar, yürütülen süreçler ve yapılan anlaşmaların en önemli kanıtı e-belgeler olacaktır. Elektronik ortama aktarılan belge ve verilerin kontrolü ve yönetimi, geleneksel yönetim metotlarından çok daha farklı olan, Elektronik Belge Yönetim Sistemi ile mümkün olabilmektedir. Belge yönetimi, örgütlerin faaliyetlerini yürütürken ürettikleri, organizasyon dışına çıkardıkları veya dışarıdan organizasyon içerisine dahil ettikleri her türlü belgenin tasnifi, dağıtılması, dosyalanması, arşivlenmesi ve imha edilmesi gibi belge üzerinde çeşitli tasarrufların yapılmasını sağlayan bir yönetim idare sistemi veya yazılım programıdır. Bu yönetim sistemi veya yazılımı içerisinde en önemli nokta verinin güvenliğinin sağlanması aşamasıdır. E-Belge yönetimi aşamasında saklanan belgelerin kullanım ömürleri boyunca içerik, format ve belge özelliklerinin korunmasının E-imza olmadan gerçekleştirilmesi çok zordur. E-Devletin sağlayacağı faydalar arasında bulunan şeffaflık ve hesap verilebilirlik sayesinde vatandaş olarak ulusal bilgi ve belgelere erişim, eskiye nazaran daha etkin ve kolay olacaktır. Bu durum iyi planlanmış etkin bir belge yönetim stratejisini zorunlu kılmaktadır. Geleneksel devlet anlayışında bilgi ve belgeye erişim, kamu personeli aracılığıyla yapılmakta ve bu işlemler sırasında tüm sorumluluk bu personelin üzerinde olmaktayken, E-Devlette vatandaş ile erişilmek istenen bilgi ve belge arasında herhangi bir aracı olmayacaktır. E-Devlet çatısı altında işlerlik kazanacak olan EBYS üzerindeki evrak ve belgelerin güvenliğinin, bütünlüğünün korunması, yetkisiz kullanımlarının engellenmesi e-imza teknolojileri sayesinde sağlanabilinmektedir (Altın, 2008: 280-285).

E-imza, kanunla ayrı tutulan işlemler haricinde gerçek hayatta ıslak imza ile yapılan her işin e-ortam üzerinden güvenilir bir şekilde yapılmasına imkan sağlamaktadır. E-imza, imzayı atacak kişiye özel olarak verilmiş anahtar sayesinde, imzalanacak olan belgenin bir takım dijital işlemlerden geçirilmesi sonucunda oluşturulan ve imzalanacak belgeye eklenen bir veri sayesinde kişi ile imzalanan belge arasında ilişki kurar. E-imza işleminin sağlıklı bir şekilde kullanılabilmesi için bu

sistemi ihtiva eden diğer yazılımlara da ihtiyaç vardır. İmzalanacak belgelere eklenen e-imza değerinin oluşturulmasında elektronik sertifika kullanılır. E-sertifika sağlayabilmek için ESHS'ye başvurmak gerekmektedir. Türkiye'de e-sertifikaların geçerlilik ömürleri en fazla 10 yıl olacak şekilde belirlenmiştir. Türkiye'de kamu kurum ve kuruluşları için yetkili kurum TÜBİTAK'a bağlı UEKAE'dir. Özel kurum ve kişilerin başvuracağı özel şirketler de mevcuttur. Sertifika sağlayıcılarından sağlanan sertifika ile kullanılan e-imza sertifika sahibini elektronik olarak imzalamış olduğu her türlü işten mesul tutar (Altın, 2008: 285-287).

4.2.2. Şifreleme Teknolojileri

Özellikle bilgi/veri'nin işlenmesi ve bir noktadan başka bir noktaya aktarılması esnasında, günümüz kamu kurum ve kuruluşlarının sıkça başvurduğu yöntemlerden bir tanesi de, verinin değişik algoritmalar ile birlikte kriptolanmasıdır. Gönderici tarafından özel bir kodla birlikte bir algoritma dahilinde şifrelenen veri, hedeflenen iletişim noktasında ulaştığında benzer bir algoritma ile kripto çözümlemesi yapılarak kullanılır. Kripto veya değişik şifreleme araçlarındaki amaç verinin iletişim ortamındaki seyahati boyunca güvenliğinin sağlanmasıdır.

Kriptoloji, Türk Dil Kurumu tarafından "Gizli yazılar, şifreli belgeler veya incelenmesi" şeklinde açıklanmaktadır (www.tdkterim.gov.tr, 25.12.2012). Bir bilim dalı olarak kabul edilen kriptoloji kendi içerisinde farklı alanlara ayrılmaktadır. Steganografi aktarılacak bilgiyi şifrelemeden gizleme yöntemiyken, Kripto Analiz şifrelenmiş bir veriyi çözme ile ilgilenir. Araştırmamda kriptoloji bilim dalının bilgi/verilerin şifrelenmesi ile ilgilenen dalı olan Kriptografi üzerinde durmak istiyorum. Bilgi/Verinin şifrelenmesini sağlayan algoritmalar da kendi içerisinde yapısına göre üç başlığa ayrılmaktadır;

4.2.2.1 Açık Anahtarlı Şifreleme

Açık anahtarlı şifrelemeye örnek olarak bilgi sistem ağlarında güvenli bağlantı kurma aracı olarak kullanılan SSH (Secure Socket Layer – Güvenli Soket Katmanı)

örnek gösterilebilinir. Açık anahtarlı şifrelemede Veri/Bilgi'yi şifrelemek amacıyla farklı, çözme amacıyla farklı anahtar kullanılır. Kullanılan bu anahtarlardan biri gizli diğeri açık anahtar olarak tanımlanır. Veriyi şifreleme amacıyla kullanılan açık anahtar erişime açık iken, şifrelenmiş veriyi çözmeye yarayan gizlidir. Açık anahtarla şifrelenmiş bir Veri, bilgi iletişim ortamında ele geçirilse dahi gizli anahtar olmadığından dolayı verinin elde edilmesini engellemektedir.

4.2.2.2 Anahtarsız Şifreleme

Anahtarsız şifreleme metodunda şifrelenmiş Bilgi/Veriyi çözmek için genel bir anahtarın bulunmamaktadır. Bir başka tabirle anahtarsız şifreleme, oluşturulan şifreleme işlemini şifrelenecek veri için özel olarak üreten algoritma türüne verilen addır.

4.2.2.3 Simetrik Şifreleme

Veri/Bilgi'yi hem şifrelerken hem de çözerken aynı algoritmanın kullanılmasıyla oluşturulan şifreleme tekniğine simetrik şifreleme denilmektedir. İletişim içerisinde bulunan her iki nokta da aynı algoritma ile şifreleme ve çözümleme yeteneğine sahip olabilmektedir. Simetrik şifreleme yukarıda bahsedilen açık anahtarlı şifreleme tekniklerine nazaran daha hızlı bir şifreleme tekniği sağladığından anlık ve hızlı bilgi paylaşımlarında tercih edilmekle beraber, anahtarın aynı olması sebebiyle ve veri iletişiminde anahtarı da beraberinde ilettiği için daha riskli olarak değerlendirilmektedir (Baliç, 2014).

4.3. Siber Güvenlik Kavramı;

Bu bölümde; siber güvenlik kavramının tanımı ve öneminden sonra hedefi ve amaçları üzerinde durulmuştur.

4.3.1. Siber Güvenliğin Tanımı ve Önemi

Siber Güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan araçlar, yöntemler, kavramlar, güvenlik politikaları ve faaliyetleri ile kullanılan teknolojiler bütünü olarak tanımlanmaktadır (Itu, 2008: 12).

Bir başka tanımıyla siber güvenlik; Elektronik haberleşme ortamını kullanan kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak ve muhafaza etmek amacıyla alınan her türlü önlem, politika ve kararlar ile kullanılan yaklaşım ve araçların bütününe denilmektedir (Bilişim Ajandası, 2011).

ABD Başkanı Sn. Obama siber güvenliğin önemine binaen 29 Mayıs 2009 yılında yapmış olduğu bir konuşmada "Siber güvenlik, ülke olarak karşılaşılan çok ciddi ekonomik ve ulusal güvenlik sağlama hedeflerinden birisi olup hükümet veya ülke olarak henüz tam anlamıyla önlem alamadığımız bir husustur." demiş ve yine aynı açıklamasında ABD Başkanı Sn.OBAMA "Amerika'nın dijital altyapısını kapsamlı olarak güven altına alma yaklaşımlarının geliştirilmesi ve bilgi ile haberleşme altyapısının savunulmasına yönelik olarak federal çözümlerin gözden geçirilmesi" gerektiğini belirtmiş ve Mayıs 2009 yılında ise "21. yüzyılda Amerika'nın ekonomik zenginliği, siber güvenliğe bağlı olacaktır." açıklamasını yaparak siber güvenliğin önemini vurgulamıştır (www.whitehouse.gov 13.01.2013).

T.C.Ulaştırma Bakanı, Sn. Binali YILDIRIM ise Siber Güvenliği "Siber savaş tehdidine karşı hazırlıklı olmanın, kurumların bilgi sistemi güvenliği olaylarına müdahale yeteneği ile kurumlar arası koordinasyon yeteneğini tespit ederek, alınacak önlemler ve bilincinin arttırılmasını amaçlamak" olarak tanımlamıştır (Sağıroğlu, 2013: 21).

Siber güvenliğin önemine dair birçok bilim ve devlet adamının yapmış olduğu açıklamaların yanında, yaşanan siber saldırılar, toplumun büyük bir kısmının dikkatini çekmiştir. Toplum nazarında artık bir siber saldırı ve savaş olgusu oluşmuştur. Bilişim teknolojilerinin günümüzde ulaşmış olduğu nokta itibariyle, fiziki sınır ve kuralların ötesinde bir başka boyutun ortaya çıktığı ve "Siber Uzay" olarak ifade edilen bu olgunun, bir söylenti veya bir tasarım olmaktan öteye gittiği ve sanallıktan gerçeklik haline geldiği artık açık olarak görülmektedir. Dünyada neredeyse tüm hizmet ve faaliyetler bu Siber Uzay içinde gerçekleşmektedir (Alkan vd., 2012: 4).

4.3.2. Siber Güvenliğin Hedefleri ve Amaçları

Siber güvenliğin en temel hedefi: Devlet, kurum ve kuruluşlarının ulusal bilgi varlıkları ve kaynakları sayılan, elektronik ortamdaki bilgi ve servislerinin, hedeflenen amaçlar doğrultusunda, insan, finans, teknik ve bilgi değerlerini dikkate alarak, korunmasını ve muhafaza edilmesini, bilgi ve verilerin yetkisiz ellere geçmesini önleyerek, bilgi bütünlüğü oluşturmaktır (Itu, 2011: 5).

4.3.3. Siber Güvenlik Tehditleri

Gerek kişisel yaşamımızda gerekse devlet işleri ile ilgili olsun hayatımızın hemen hemen her alanında bilgi sistem teknolojilerini kullanıyoruz. Alış-Veriş, Bankacılık, Su ve elektrik işleri, Sağlık, Eğitim, Trafik düzenlemeleri gibi en temel ihtiyaçlarımızın karşılanmasında bilgi iletişim teknolojilerinin kolaylıklarından faydalanıyoruz. Bilgi işlem teknolojilerine olan bağlılığımız bu sistemlerin kısa süreli dahi olsa servis dışı kalması durumunda, bireysel anlamda vatandaşların hizmetten mahrum kalmasına, ulusal anlamda ise büyük finansal kayıpların yaşanmasına sebep olmaktadır. Herhangi bir internet bağlantısı üzerinden erişilebilen bu sistemler siber saldırıların artmasına ve saldırıyı yapanların kolayca kimliğini gizleyebilmelerine imkân sağlayabilmektedir. Siber saldırılar zaman ve mekan ayırımı olmaksızın planlı veya plansız, organize veya bireysel olarak her an yaşanabilmekte ve toplum yaşamını tehdit etmektedir. Günümüz bilgi sistem dünyasında isim yer etmiş Google, Sony, Lockheed Martin, PBS, Epilson ve son olarak City Bank gibi büyük teknolojik şirketler dahi tam anlamıyla güvenlidir denilemez. Dünya üzerindeki siber saldırıların çoğu, yasal düzenlemelerin az yada olmadığı ülkeler üzerinden gerçekleştirildiğinden, saldırı ve hırsızlığın yapısı itibariyle hızlı bir şekilde yapılması, saldırganların yakalanmasını güçleştirmektedir. Siber suçlarla mücadele anlamında uluslararası iş birlikteliğinin henüz kurulamamış olması, siber suçlarla mücadelenin giderek artacağı kaygısını da beraberinde getirmektedir (Itu, 2011).

4.3.4. Siber Saldırı Yöntemleri

Kamusal kurum ve kuruluşlara veya özel sektördeki şirketlere yönelik, kişi, gurup veya ülkeler tarafından yapılan siber saldırıları, kullanılan yöntem ve metotları bakımdan, genel anlamda üç ana başlık altında toplamak mümkündür. Siber saldırılar bu metotların birini veya koordineli bir şekilde birkaçını kullanarak yapılabilmektedir. Bu saldırıları en genel anlamda Fiziksel Hasar ve Tahripler, Elektromanyetik Titreşim, Bilgisayar ve Ağ Sitemlerine Yapılan Saldırılar olarak başlıklandırabiliriz (Saalbach, 2013: 11).

4.3.4.1. Fiziksel Hasar ve Tahripler

Bilgisayar sistemlerine, iletişim hatlarına ve bilgi sistem ağlarına yapılan fiziksel hasar ve tahrip amaçlı saldırılar genelde sabotaj tekniği kullanılarak yapılan donanım, kablo, anten sistemleri ve uydular üzerine gerçekleştirilen sistemi imha amacı taşıyan saldırılardır. Asıl amacı bilgi ve belge kaçakçılığından ziyade, sistemin çalışamaz hale getirilmesini amaçlamaktadır. Fiziksel bina, oda, evrak güvenliği ile Personel Güvenliğini, terinde ve zamanında uygulamak koşulu ile bu tarz saldırılardan korunmak veya hasar etkisini en aza indirebilmek mümkündür (Saalbach, 2013: 11).

4.3.4.2. Elektromanyetik Titreşim / Pals (EPM)

Günümüzde kullanılan modern elektronik cihazların en temel birimini oluşturan transistörlerin, meydana getirilen yüksek yoğunluklu elektromanyetik titreşimlerle bozulması ve servis dışı kalmasını sağlayan bu tarz saldırılar, en etkili siber saldırılar olarak nitelendirilmektedir. Atom bombasının patlatılması neticesinde de elektromanyetik titreşim oluşturulabilmektedir. Teknik olarak, elektromanyetik titreşimden korunmak mümkün olsa bile, korunma yollarının pahalı olmasından dolayı tüm sistemlerin korunaklı hale getirilmesi maliyet/etkin değildir (Saalbach, 2013: 11).

4.3.4.3. Bilgisayar ve Ağ Sistemlerinin Manipüle Edilmesi

Siber saldırı yöntemleri arasında bulunan bu saldırı metodu en sık ve en kolay tatbik edilebilmesi bakımından en çok karşılaşılan saldırı şeklidir. Bilgisayar ve ağ ortamına yerleştirilebilecek ufak bir yazılım veya virüs ile kolay bir şekilde sistem manipüle edilebilmektedir. Çoğu zaman ağa bağlı tek bir bilgisayarın yeterli olduğu bu saldırılarda, ABD-İran Siber Savaşı (Stuxnet)'nda da görüldüğü üzere bağımsız, internete veya herhangi bir ağa bağlı olmayan sistemlere de saldırılar düzenlenebilmektedir (Saalbach, 2013: 11). Bu yöntemi kullanarak yapılan siber saldırı yöntemlerinden bazıları aşağıda açıklanmıştır.

Hizmetin Engellenmesi Saldırıları (DoS, DDoS); İki türü vardır DoS (Denial of Service) yani hizmet veren sistemleri veya servisleri aşırı yoğun tutmak suretiyle isteklere cevap veremez hale getirmek ve böylelikle servislere ihtiyacı olan gerçek kullanıcıların hizmet alabilmesini engelleme saldırılarıdır. DoS saldırılarının, farklı saldırı noktalarından daha karmaşık halde yapılmasını sağlayan DDoS (Distrubuted Denial of Service) yani dağıtık servis engelleme saldırıları da bulunmaktadır. Hizmeti sekteye uğratma saldırıları genellikle sahte IP adresleri üzerinden yapıldığından, saldırganı ortaya çıkarmak zordur. Saldırı süresince hizmet verilen internet sitesinin bant genişliği, gerçek olmayan fakat işlenmesi ve cevaplandırılması zaman alan internet paketleri ile meşgul edilir. Bir tek korsanın eşgüdümlü korsan bilgisayarlar üzerinden aynı anda birden fazla bilgisayar ile aynı adrese yönelik başlatabileceği bu saldırı türü en yaygın ve en etkin siber saldırı türüdür. Amaç bilgi veya belge hırsızlığından ziyade hizmeti servis dışı bırakmaktır. Gürcistan ve Estonya siber saldırılarında da bu yöntem kullanılmıştır. Teknik olarak bant genişliğini saldırı miktarının üstünde tutabilmekle saldırıdan etkilenmeden devlet veya özel sektör uygulamaları hizmetlerini devam ettirebilmektedirler. DDoS saldırıları altyapısı yeterli olmayan sistemleri çok kolay servis dışı bırakabilir (Önal, 2013).

Bilgisayar Virüsleri; Temelde çalıştırılabilir küçük programlar olan bilgisayar virüsleri, etki ettiği bilgisayara varlıklarını hissettirmeden çalışabilen, bulunduğu sistemde hızla çoğalıp yatay veya dikey sistemlere geçiş yapabilen programlardır.

Amacına ve saldırı şekline göre sistemi yavaşlatan, istenmeyen şekilde çalıştıran, nispeten zararı sınırlı virüs programları olduğu gibi, etkilediği sistemlerdeki dosyaları kullanılamaz hale getirebilen, hatta fiziksel ısınma veya aşınma ile sistemin çalışmamasına sebep olabilen değişik tür ve biçimde bilgisayar virüsleri mevcuttur. Çeşitlerine göre virüsler ve diğer bazı yazılımlar şöyledir (Bilim ve Teknik Dergisi, 2005: 3).

Dosya Virüsleri; Bilgisayar ortamında çalıştırılabilir dosya türleri olan COM, EXE, DRV, DLL, BIN, OVL, SYS uzantılı dosyalara bulaşarak, bu dosyalar çalıştırıldığında bellek üzerinden kendilerini başka dosya veya sistemlere kopyalamaya çalışan zararlı bilgisayar programlarıdır.

Açılış (Boot) Virüsleri; Sistem veya disketlerin açılış aşamasında bilgisayar tarafından gözden geçirilen, açılış sektörüne yerleşen bu virüsler sistemlerin açılmamasına, disklerin veya disketlerin bozulmasına sebep olmakta ve böylelikle veri kaybı yaşanmaktadır.

Truva Atı (Trojan); Kullanıcının bilgisayarına gizlice yerleşerek, sistemin dışarıdan müdahalelere açık hale gelmesini mümkün hale getirerek, kötü niyetli kişilerin bilgisayarın kontrolünü ele geçirmesine imkan sağlayan programlardır.

Solucan (Worm); Sisteme virüs veya trojan yazılımını gizli olarak taşıyan dosyalara verilen isimdir (Sağıroğlu, 2013: 64). Etki ettikleri savunmasız ve korunaklı olmayan sistemleri kolaylıkla devre dışı bırakabilen bu virüs türlerini çoğaltmak mümkündür. Siber güvenliğin sağlanmasında en temel ve ilk adım olan sistemin ve o sisteme bağlı işlem yapan bilgisayarların virüslere karşı korumalı olması gerekmektedir. Bu da kullanılabilecek bir anti-virüs yazılımı ile sağlanabilir.

4.3.5. Siber Güvenliği Sağlamak İçin Alınan Önlemler

Bilişim toplumunda ekonomik, sosyal, kültürel ve siyasi açıdan gücü temsil eden bilginin hızlı ve kolay bir şekilde, işlenmesini, paylaşılmasını, saklanmasını ve

dağıtılmasını sağlayan İnternet ile birlikte bilgi sistem teknolojileri de hızla gelişmektedir. Bu gelişim bir yandan devletlerin ve bireylerin hayatlarını kolaylaştırırken, diğer yandan hayatı zorlaştıran pek çok siber tehdidin oluşumuna da zemin hazırlamaktadır. Bilgi toplumu dönüşümü ile başlayan ve halen gelişmekte olan E-Devlet uygulamaları ve hizmetlerinin güvenliğinin sağlanması ve bu hizmetlere bağımlı hale gelen kritik altyapıların korunması, tüm dünyanın gündemindedir (Bil.Tek.Koor.D.Bşk.lığı, 2009).

Siber tehdidin, esasında gözle görülmez ve hızla gelişen bir yapıya sahip olması sebebiyle, tehdidin tanımlanmasında ve tam olarak nereden nasıl bir şekilde karşılaşılacağı ile ilgili bir bilinmezlik hâkimdir (Bıçakcı, 2012: 221). Siber savaşın varlığını ve olası olası tehdit ve tehlikelerini ciddiye alarak hazırlanmaya başlayan ülkeler kara, deniz, hava ve uzaydan sonra beşinci bir askeri kuvveti de devreye sokmanın mücadelesini vermeye başlamışlardır (Alkan, 2014).

Başlangıçta bireysel ve tekdüze yapılan siber saldırılar günümüzde yerini yavaş yavaş sistematik yapılanmaya bırakmaktadır. Askeri anlamda bu yapılanmaların örneklerini verecek olursak, ABD Deniz Kuvvetleri yılda 24.000 askerini bilgi güvenliği konularında eğitmektedir. ABD Hava Kuvvetleri ise Nevada Hava Üssünde gerçekleştirdiği ve Haziran 2012 tarihinde ilk mezunlarını vermiş olan bir eğitim ile birlikte, kursiyerlere siber saldırılardan nasıl korunulacağı ve önlenebileceği ve karşı siber saldırıların nasıl yapılabileceği konularında eğitim vermektedir. Bu eğitimlerle birlikte başlayan süreç içerisinde ABD Hava Kuvvetlerinden 17 Subaya Siber Muhabere Subayı tecrübesi kazandırılmıştır. 2011 yılında Çin hükümetinin yayımlamış olduğu rapor doğrultusunda 30 Siber Uzmanın Mavi Ordu adı altında Guangdong siber eğitim üssünde eğitildiği açıklanmıştır. Rusya Savunma Bakanlığı 2012 yılında, anti-virüs programlarını, ateş duvarlarını ve buna benzer güvenlik önlemlerini ortadan kaldırmanın/aşmanın metotlarını içeren bir dizi eğitime başlamıştır. Rusya'da her yıl, yetenekli korsanların bulunup devlet adına çalışmaları amacıyla, korsan yarışmaları düzenlenmektedir. İsrail medyasının yayımlamış olduğu haberlere göre, İsrail ordusunda yeni bir bölüm olarak teşkil edilen "Saldırgan" birliklerinin amacı hasım kuvvetleri uzaktan siber saldırı ile etkisiz hale getirmek olarak tanımlanmış ve bu doğrultuda asker istihdamı yapılmıştır. İsrail'de 2012 yılında ilk mezunlarını veren siber

eğitim gerçekleştirilmiştir. Yine İsrail'de askeri personel ve sivil korsanlar tarafından organize edilen siber korsanlık yarışmaları düzenlenmektedir (Saalbach, 2013: 11).

Günümüzde, çoğu ülke ve uluslararası kuruluşlar, siber güvenlik konusunda ülkelerarası bilgi paylaşımı, teknik boyutta sürdürülen çalışmalara destek verilmesi, siber güvenlik farkındalığının arttırılması ve uluslararası işbirliğinin sağlanması konularında çalışmalar yürütmektedirler. NATO, AB, BM, ABD ve Türkiye tarafından siber güvenliğin sağlanması ve farkındalığının kazanılması adına yürütülen çalışmalar ve atılan adımlar aşağıda açıklanmıştır;

4.3.5.1. NATO'da Siber Güvenlik Algısı ve Alınan Önlemler

Soğuk savaşın sona ermesinden sonra uluslararası sistemin güvenlik algısı da bununla birlikte değişime uğradı. NATO'nun 1991 yılında yayınlanan stratejik belgesiyle birlikte soğuk savaş dönemindeki büyük, yekpare ve potansiyel açıdan var olan tehditlerinin çoğunun ortadan kalkması sonucu NATO yeniden yapılanmaya başladı. Soğuk savaş sonrasındaki dönemde, geleneksel savaş taktikleri yerine, asimetrik savaş yöntemleri öne çıktı. Yaşanan etnik çatışmalar, sınır anlaşmazlıkları, organize suç örgütleri ile mücadele gibi değişen savaş yöntemleri ve araçları soğuk savaş döneminin dinamiklerine cevap vermek üzere organize edilmiş olan NATO'nun değişen güvenlik algısına cevap verip veremeyeceği tartışmasının doğmasına sebep olmuştur. Kosova çatışması sırasında, NATO bombardımanına Sırp bilgisayar korsanları tarafından siber saldırılarla karşılık verilmiştir. Kısacası soğuk savaş sonrası NATO uluslararası sistemdeki güncel tehditleri de kapsayacak, yeni bir siber savunma stratejisi inşa etmeye başladı. NATO, 1999 Lizbon Zirvesinde siber savunma ve kritik bilgi altyapısının korunmasını da içeren yeni stratejinin hazırlanmasına onay verdi. Bu yeni strateji değişikliği ile NATO geleneksel savaş imkânlarını bırakmadan yenilerine sahip olma amacıyla, siber savunmayı da içeren hibrit savaş stratejisini başlattı ve bu yaklaşımı bütün üye ülkelerinde uygulamaya başladı. Üye devletlerin siber sistemlerine yapılacak herhangi bir saldırının, ülkedeki güvenliği derinden sarabileceği gibi endişeler, 21 Kasım 2002'de düzenlenen Prag Zirvesi'nin gündemine yansıdı. Zirve'de siber saldırılara karşı savunmanın güçlendirilmesi konusu ele alındı ve NATO'nun gerekli planlamaları yapması karara bağlandı. Zirve'de alanına karar doğrultusunda

NATO Ağ ile Etkinleştirilmiş Güç (Network-Enabled Capability-NNEC) programı başlatıldı. Akabine NATO İletişim ve Enformasyon Sistemleri Ajansı (Communications and Information Systems Agency-NACISA) ve Avrupa İttifak Güçleri Büyük Karargâhı (Supreme Headquarters Allied Powers Europe-SHAPE) Teknik Merkezi, yerlerini 1 Haziran 1996'da kurulan NATO Danışmanlık, Komuta-Kontrol Ajansı'na (NATO Consultation, Command and Control Agency-NC3A) bıraktı. Bu ajansın temel görevi, teknolojik gelişmeleri takip ederek, bunların NATO bünyesinde işlevsel hale gelmesini sağlamak ve NATO'nun askeri operasyonlar sırasında duyduğu ihtiyaçlara cevap verebilmektedir. NC3A, NATO operasyonlarında araştırmadan takibe, hava komuta-kontrolden füze savunmasına, uydu kontrol ve telsiz sistemlerinden elektronik harbe, erken uyarı ve kontrol sistemlerinden, iletişim-bilişim sistemlerine kadar birçok sahada görev yapmaktadır. NC3A yapılanması içinde siber güvenlik ve bilgi paylaşımının sağlanması için faaliyet gösteren bir bölüm de bulunmaktadır. NATO'nun 2008 Bükreş Zirvesinde siber güvenlik konusu kapsamlı bir biçimde ele alınmış ve siber güvenlik kapsamında yapılması gereken dönüşüm için gerekli kaynakların temin edilmesi kararlaştırılmıştır. Yine aynı zirvenin sonuç bildirgesinde ittifak ülkelerinin bilgi sistemlerinin siber saldırılara karşı güçlendirilmesi için NATO'nun kararlılıkla çalışacağı belirtilmiştir. Brüksel Zirvesi sonrasındaki yapılan çalışmalar sonunda NATO Brüksel'de Siber Savunma Yönetimi Otoritesi (Cyber Defense Management Authority-CDMA) ile Estonya Tallinn merkezli NATO Siber Savunma Mükemmelliyet Merkezi (Cooperative Cyber Defence Centre of Excellence–NATO CCDCOE) kurulmuş ve halen aktif olarak görevine devam etmektedir (Bıçakcı, 2012: 206-208).

NATO'nun yeni savaş anlayışı doğrultusunda elektronik harp merkezleri de yeniden düzenlendi ve 7 Eylül 2004'te NATO İletişim ve Enformasyon Sistemleri Servisi Ajansı (NATO Communication and Information Systems Services Agency-NCSA) oluşturuldu. 2004 yılında kurulan bu ajansın temel görevi, merkez karargâhı ile diğer görev güçleri arasındaki iletişimi sağlamaktır. Siber saldırılar ilk olarak iletişim kanallarına odaklanmaktadır. Prag Zirvesi'nde alınan kararlardan bir diğeri de kritik alt yapıların terörizme karşı korunması için NATO siber savunma programının oluşturulması idi. Bu yüzden NCSA siber saldırılara karşı ilk müdahaleyi yapacak unsur olarak belirlenmiştir. Ajansın içindeki merkezlerden en önemlisi, muharip unsurların bilgi güvenliği ve ittifak genelinde güvenli iletişimi sağlamakla yükümlü NATO Bilgi

Güvenliği Teknik Merkezidir (NATO Information Assurance Technical Centre-NIATC). NIATC, bilgisayar ağlarını Bilgi Güvenliği Operasyon Merkezi ve NATO Bilgisayar Olayları Müdahale Gücü Teknik Merkezi'yle (NATO Computer Incident Response Capability Technical Centre-NCIRC) işbirliği içinde ve sürekli olarak takip etmektedir. Bu gelişmeye müteakip 2006'da yapılan Riga Zirvesi'nde ağ ile güçlendirilmiş komuta-kontrol kavramı üzerinde durulmuş ve bilişim alt yapısının savunmasının iyileştirilmesinin gerektiğine vurgu yapılmıştır. Bütün bu girişimlere rağmen siber uzay da tehdit düzeyinin artması ve siber araçlarla saldırının çok küçük eğitimlerle gerçekleştirilebildiği gerçeği halen NATO üyelerini korkutmaktadır (Bıçakcı, 2012: 213-214).

Haziran 2011 yılında incelenen siber savunma politikasında, NATO'nun başlıca siber savunma politikaları olarak;

- Siber savunmanın NATO'nun yapısına entegre edilmesi, NATO'nun temel görevlerinin planlanmasında siber savunmanında yer alması gerektiği,
- Teşkilat olarak NATO'nun, herhangi bir üyesine karşı gerçekleştirilebilecek siber saldırıları önlemeye ve savunmaya odaklanması gerektiği,
- NATO'nun kendi bilgi sistem ağlarını koruması amacıyla güçlü bir siber savunma merkezinin geliştirilmesi gerektiği,
- Ulusal kritik ağların korunmasında asgari güvenlik önlemlerinin alınmasının sağlanması,
- Üye ülkelerin siber savunma kapasitelerini arttırabilmek ve ulusal kritik altyapılarının zayıf yönlerini giderebilmeleri için teşkilat olarak asgari seviyede siber savunma yardımının sağlanması gerektiği,
- Siber güvenliğin başarılmasında uluslararası kuruluşlar, özel sektör ve diğer ortaklar (AB, BM gibi) ile bağlantıların kurulması gerektiği belirtilmiştir (Bıçakcı, 2012: 221).

4.3.5.2. Avrupa Birliği Bilgi Toplumu Vizyonu ve Eylem Planları

AB tarafından, siber güvenliğin sağlanmasına yönelik 1995 yılından beri yayımlanan temel direktiflerin bazıları aşağıda sıralanmıştır;

- 1995/46/EC sayılı Kişisel Verilerin Korunması Direktifi,
- 1999/93/EC sayılı Elektronik İmza Direktifi,
- 2000/31/EC sayılı Elektronik Ticaret Direktifi,
- 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Gizliliğin Korunması Direktifi,
- 2006/24/EC sayılı Kamusal Elektronik Haberleşme Hizmetlerinin Sunumu Sırasında veya Kamusal Haberleşme Şebekeleri Üzerinden Elde Edilen Verilerin Muhafazasına İlişkin Direktif,

Yayımlanan bu direktiflerin yanında, AB organlarının almış olduğu bazı önemli tavsiye kararları şunlardır;

- Avrupa Komisyonu tarafından, 25 Ocak 1999 tarihli, küresel ağlarda yasadışı zararlı içerik ile mücadele etmek suretiyle internetin güvenli kullanımını amaçlayan kamusal eylem planı oluşturulmasına dair tavsiye kararı,
- Avrupa Birliği Konseyi tarafından, 24 Şubat 2005 tarihli, bilgi sistemlerine yönelik saldırılara ilişkin çerçeve kararı, (Bu çerçeve karar üye ülkeleri, bilgi sistemlerine ve bilgiye yetkisiz müdahale ve erişim fiillerinin, suç olarak kabul edilmesine zemin oluşturacak bir sistemin tesisi ile bu fiillerin etkin, makul ve caydırıcı şekilde cezalandırılması amacıyla 7 gün 24 saat ulaşılabilir temas noktaları oluşturmaya çağırmaktadır.)
- Avrupa Birliği Konseyi tarafından 22 Mart 2007 tarihli Avrupa'da güvenli bir bilgi toplumu oluşturma eylemine ilişkin tavsiye kararı,

Yukarıda değinilen temel kararların dışında AB, siber güvenliğin sağlanması ve altyapıların korunması için alınması gereken yasal, teknik ve idari tedbirleri belirlemek amacıyla, Bilgi Toplumu Teknolojileri ve Avrupa Güvenlik Araştırma Programı, Kritik Altyapıları Araştırma Koordinasyon Projesi, Avrupa Kritik Altyapıların Korunması Programı gibi çeşitli proje ve programları da yürütmektedir. Bu programlar sayesinde, AB dahilinde, siber tehditler, kritik altyapılarda bulunan açıklar, var olan risklere karşı alınabilecek tedbirler ve izlenebilecek stratejiler hakkında bilgi paylaşımı faaliyetleri yerine getirilmektedir. Türkiye'nin de aralarında bulunduğu 47 üyesi bulunan Avrupa

Konseyinin, siber güvenlik konusunda yürüttüğü en önemli çalışma Avrupa Konseyi Siber Suç Sözleşmesi (Council of Europe Convention on Cybercrime)'dir. 2001 yılında Budapeşte'de imzaya açılan ve 2004 yılının Temmuz ayında yürürlüğe giren bu sözleşme, internet ve diğer ağ ortamları yoluyla işlenen suçlarla mücadele konusunda uluslararası boyutta atılmış ilk ve en önemli adımdır. Bu sözleşmenin temel hedefi, gerekli olan yasal tedbirlerin alınmasını sağlamak ve uluslararası işbirliğini teşvik etmek suretiyle toplumun siber suçlara karşı korunmasını sağlamaktır. Bu sözleşmeye taraf olan ülkeler, sözleşmede suç olarak belirtilen fiillerin, kendi ulusal mevzuatlarında da suç olarak tanımlanmasını sağlamayı ve bu suçların soruşturulması için gerekli tüm yasal tedbirleri almayı kabul etmektedirler. Avrupa Konseyi Siber Suç Sözleşmesi siber suçları dört ana başlıkta sınıflandırmıştır. Bunlar; bilgisayar sistemlerinin ve bilginin gizlilik, bütünlük ve erişilebilirliğini hedef alan suçlar, bilgisayar ile ilgili suçlar, içerikle ilgili suçlar, telif ve benzeri hakların ihlali ile ilgili suçlardır. Bu önemli yasanın dışında, Avrupa Konseyi tarafından 28 Ocak 1981'de "Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme" (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) kabul edilmiştir. Avrupa Konseyi üyesi olmayan ülkelerin de katılımına açık olan sözleşme, gerek kamu sektöründe, gerekse özel sektörde geçerli olmak üzere verilerin korunması alanında kabul edilmiş olan uluslararası hukukun ilk bağlayıcı sözleşmesidir (Bil.Tek.Koor.D.Bşk.lığı, 2009: 19-24).

4.3.5.3. Birleşmiş Milletler'in Çalışmaları

İkinci dünya savaşı sonrası, barışı korumak ve uluslararası ilişkileri düzenlemek amacıyla 1945 yılında kurulan Birleşmiş Milletler, kuruluş amacının yanında, çevre konularında, çocuk gelişimi ve sağlığı, insan hakları, tarımsal kalkınma, yoksullukla mücadele ve ekonomik kalkınma, eğitim, kadın hakları, atom enerjisinin barışçıl amaçlarla kullanılması gibi pek çok alanda çalışmalarını sürdürmektedir. Birleşmiş Milletler, 1980'lerin sonlarından itibaren başlattığı siber güvenlik faaliyetlerine, günümüzde de halen devam etmektedir. BM, siber güvenlik konusunda faaliyetlerini, BM Genel Kurul kararlarının yanında, BM Bilgi ve İletişim Teknolojileri Görev Gücü ve BM ajansı olan Uluslararası Telekomünikasyon Birliği (ITU) eliyle yürütmektedir.

BM Bilgi ve İletişim Teknolojileri Görev Gücü, Kasım 2001'de BM Ekonomik ve Sosyal Konseyi'nin talebi üzerine kurulmuş, BM kalkınma hedeflerine ulaşma konusunda faaliyetlerini sürdüren bir birimdir. Yayınlamış olduğu kılavuz yayınlarla, BM adına bilgi güvenliği konusunda alınması gereken çözümleri, güvenlik olaylarına müdahale mekanizmalarını ve siber ortam güvenlik stratejilerini belirlemektedir. Söz konusu kılavuzlar, BM adına siber ortamda güven ve güvenliğin sağlanabilmesine yönelik uygulamaları ve standartları içermektedir. Merkezi İsviçre'nin Cenevre kentinde bulunan Birleşmiş Milletler'e bağlı bir ajans olarak faaliyetlerini yürüten Uluslararası Telekomünikasyon Birliği (ITU), esas olarak Bilgi İletişim Teknolojileri konularında çalışmalar yürütmekte, kamu ve özel sektör kuruluşlarına Bilgi ve İletişim Şebekeleri alanında hizmet sunmaktadır. Başlıca görevleri arasında; Radyo spektrumunun küresel ölçekte kullanımını düzenlemek, uydu yörüngelerinin tahsisinde uluslararası işbirliğini sağlamak, farklı haberleşme sistemleri arasında bağlantılar sağlanmasına izin veren dünya standartlarını oluşturmak gibi görevlerinin yanında, siber güvenliğin sağlanması gibi güncel konularda da çalışmalar yapmaktadır. Türkiye'nin de aralarında bulunduğu, 191 devlet bazında üyesi, 700'den fazla sektör temsilcisi bulunmaktadır. Siber güvenlik konusunda dünyada etkin rol oynayan önemli bir kurumdur. 2001 yılında, ITU Konseyi, uluslararası kurum ve kuruluşları, şirketleri, sivil toplum örgütlerini ve hükümetleri, geleceğin bilgi toplumu için ortak bir vizyon belirlemek amacıyla bir araya getirmiş ve Dünya Bilgi Toplumu Zirvesi (World Summit on the Information Society -WSIS) adıyla uluslararası bir toplantı düzenlemeye karar vermiştir. BM Genel Kurulunun 56/183 sayılı kararı ile de onaylanan söz konusu zirvenin, ilk aşaması Aralık 2003'te Cenevre'de, ikinci aşaması Kasım 2005'te Tunus'ta gerçekleştirilmiştir. İnternet eksenli konuların tartışıldığı bu iki konferans sonucunda Cenevre Deklarasyonu, Cenevre Eylem Planı, Tunus Taahhütleri ve Bilgi Toplumu için Tunus Gündemi başlıklı dört doküman üzerinde mutabakat sağlanmıştır. ITU Genel Sekreterliği, Dünya Bilgi Toplumu Zirvesi sonrasında, bilgi toplumunda güven ve güvenliğin sağlanmasına yönelik uluslararası işbirliğinin sağlanması amacıyla bir model sunan "Küresel Siber Güvenlik Gündemi"ni yayımlamıştır. Yayımlanan bu bildirgede başlıca yedi ana hedef belirlenmiştir (Bil.Tek.Koor.D.Bşk.lığı, 2009: 1-11).

Bunlar;

- Küresel ölçekte uygulanabilir, mevcut ulusal ve uluslararası mevzuatlara uygun bir siber güvenlik mevzuatının geliştirilmesi,
- Küresel ölçekte kabul edilen asgari güvenlik ölçütlerinin, yazılım ve donanımsal olarak akredite edilmesi amacıyla gerekli planların oluşturulması,
- Siber güvenlik konularında çalışan ulusal ve bölgesel kuruluşların kurulması ve siber güvenlik politikalarının oluşturulması,
- Mevcut ve olası mevzuatlar hakkında, uluslararası işbirliğini sağlamak amacıyla, izleme, uyarı ve olaylara müdahale için küresel ölçekte bir model kurulması,
- Küresel bir dijital kimlik sisteminin kurulması ve bu bilgilerin tüm dünyada tanınmasını sağlayacak bir yapının kurulması,
- Sektöreler arası siber güvenlik konusunda bilgi alışverişini sağlamak üzere kurumsal kapasitenin geliştirilmesi,
- Tüm bu konular hakkında uluslararası işbirliği ve koordinasyonun tesis edilmesidir.

Tüm bu alınan kararların uygulanması ve faaliyetlerin yürütülmesinde ITU Genel Sekreterliği'ne yardımcı olmak için, siber güvenlik ile ilgili konularda yüksek düzeyde bilgili uzmanlardan oluşan bir "Yüksek Seviyeli İnsanlar Grubu" kurulmuştur. Bu grup tarafından hazırlanan Küresel Stratejik Rapor, siber güvenliğin beş ana unsurunu açıklamaktadır. Küresel siber güvenliğin beş ana unsuru Tablo 4'te gösterilmiştir.

Tablo 4: Küresel Siber Güvenliğin Beş Ana Unsuru

Küresel Siber Güvenliğin Beş Ana Unsuru				
Yasal Tedbirler	Teknik ve İşlevsel Tedbirler	Kurumsal Yapılanma	Kapasite Geliştirme	Uluslararası İşbirliği
Küresel düzeyde birlikte çalışabilir ve uygulanabilir bir güvenlik mevzuatı modeli.	Güvenlik protokolleri ve standartları, yazılım ve donanım akreditasyon planları üzerine küresel çerçeve modeli.	Kurumsal yapıların oluşturulmasında küresel stratejiler, siber güvenlik politikaları, izleme, uyarı ve olaylara müdahale, genel ve evrensel dijital kimlik sistemi.	1, 2 ve 3. Unsurlar için gereken bireysel ve kurumsal kapasitenin geliştirilmesi.	Uluslararası diyalog, işbirliği ve koordinasyon.

Kaynak: ITU, 2008.

Yine, BM Ajansı olarak çalışmalarını yürüten ITU tarafından koordine edilen, kamu ve özel sektör kuruluşlarını, sivil toplum kuruluşlarını, akademik kuruluşları bir araya getiren siber güvenlik kapısı platformu ile ITU'nun siber güvenlik konusundaki faaliyetleri hakkında bilgi ve yayınlar paylaşılmaktadır. ITI, küresel toplumun siber tehditlere ilişkin savunma, önleme ve karşı koyma kapasitesini geliştirmeyi amaçlayan, Siber Tehditlere Karşı Çok Taraflı İşbirliği (International Multilateral Partnership Against Cyber Threats/IMPACT) ile ortak çalışmalar yürütmektedir. Bu çalışmalardan bazıları;

- Siber tehditlerle ilgili küresel bilginin toplanmasına, analiz edilmesine ve paylaşılmasına,
- Küresel siber tehditlere karşı uyarı ve acil durum müdahale mekanizmalarının oluşturulmasına,

- Siber güvenliğin teknik, yasal ve politik yönleri ile ilgili çalışmalar yapılmasıdır.

Uluslararası sistemin etkin ve belirleyici bir aktörü olarak BM, gerek kendisine bağlı kurum ve kuruluşlarla, gerekse diğer kurum ve kuruluşlar ile birlikte yürüttüğü ortak çalışmalar sayesinde, uluslararası siber güvenlik çalışmalarına en fazla katkı sağlayan kurumların başında gelmektedir.

4.3.5.4. ABD ve Siber Güvenlik Stratejisi

11 Eylül saldırılarından önce A.B.D. Eski Başkanlarından George W.Bush yakın gelecekte siber teröristlerin ABD'ye karşı saldırıda bulunabileceği konusunda açıklamaları olmuştur. Başkan adayı iken yapmış olduğu konuşmada, Amerikan ordusunun kitle imha silahları, füze teknolojilerinin gelişmesi ve siber terörizmin yükselişi gibi birçok tehdit tarafından kuşatılmış olduğunu söylemiştir. 11 Eylül saldırısı sonrasında dönemin A.B.D. Başkanı George W. Bush Beyaz Saray'da Siber Güvenlik Dairesi'ni kurmuş ve başına da terörle mücadele eski koordinatörü Richard Clarke'ı atamıştır (Weimann, 2004: 3).

DARPA (Amerikan Savunma Bakanlığı İleri Araştırmalar Merkezi) projesi olarak, 1966 yılında olası bir nükleer savaş sonrası askeri birliklerin haberleşmesi amacıyla kurulan ve daha sonra üniversiteler ve günümüz de tüm dünyada kullanıma sunulan, ağlar arası haberleşme projesi olan "İnternet" sistemini ilk kuran ve geliştiren ülke olarak ABD'de siber güvenlik üzerine yapılan çalışmalar belirli bir aşamaya gelmiştir. ABD Savunma Bakanlığı'na bağlı Siber Komutanlığı'nın operasyonel kabiliyeti bulunmaktadır. Bu komutanlığın kuruluş görevi; Savunma Bakanlığı'nın bilgi sistem ağlarının korunması ve savunmasına yardımcı olmak, Savunma Bakanlığı'nın askeri operasyonlarına ve harekatlarına destek sağlamak ve gerektiğinde bu harekatları yönetmek, ABD ve müttefiklerinin siber uzayda serbest bir şekilde faaliyet göstermelerini sağlarken düşman ülkelerin faaliyetlerinin engellenmesine yönelik aktiviteleri planlama, koordine etme, senkronize etme ve yönetmek olarak belirtilmiştir. Siber güvenlik farkındalığının sağlanması ve muhafaza edilmesi adına ABD Başkanı Barack OBAMA her yılın ekim ayını Siber Güvenlik Farkındalık ayı olarak ilan etmiş

ve her yılın ekim ayında siber güvenlik farkındalığını arttırmaya yönelik etkinlikler düzenlenmesini sağlamıştır (Bakır, 2012).

ABD Beyaz Saray Başkalığı tarafından yayımlanan "Kapsamlı Siber Güvenlik Girişimi" isimli siber güvenlik konseptinde, temel olarak aşağıda belirtilen konular belirlenmiştir;

- Kamu kurumları ağlarını tek bir ağ altında güvenli internet bağlantıları ile yönetecek sistemin kurularak, genişletilmesi,
- Kamu kurumları genelinde siber saldırıları tespit eden algılayıcıların kurulması ve bu algılayıcı sistemlerinin kurulumunun sürdürülmesi,
- Ar-Ge çalışmalarının arttırılmasını koordine etmek ve yönlendirmek,
- Güvenilen internet bağlantılarının geliştirilmesi ile tek bir ağdan kamu kurumlarının hizmetlerinin yönetilebilmesinin sağlanması,
- Durumsal farkındalığı geliştirmek ve bilgi paylaşımını sağlayabilmek için mevcut siber merkezlerinin birbirine bağlanması,
- Merkezi hükümet önderliğinde karşı siber casusluk planı geliştirilmesi ve uygulanması,
- Sınıflandırılmış/Gizli ağların güvenliğinin arttırılması,
- Siber eğitim çalışmalarının genişletilmesi,
- Süregelen caydırıcılık stratejileri ve programları tanımlama ve geliştirme,
- Küresel tedarik zinciri ve risk yönetimi için çok yönlü yaklaşımların geliştirmesi,
- Kritik altyapı alanları içine alan ve devletin sorumluluklarını tanımlayan genişletilmiş siber güvenlik çalışmaları yapma olarak belirtilmiştir (www.whitehouse.gov 24.10.2012).

Yukarıdaki maddelerden de anlaşılacağı üzere, A.B.D. siber savunma ve siber güvenlik konularına oldukça önem vermekte ve siber ülke güvenliğinin sağlanması amacıyla çalışmalar yürütmektedir.

4.3.5.5. Türkiye'de Siber Güvenlik Çalışmaları ve Algısı

2012 yılı Nisan ayında Türkiye'de gerçekleştirilen Hanehalkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre; Türkiye genelinde hanelerin %47,2'si evden İnternete erişim imkânına sahiptir. Bu oran 2011 yılının aynı ayında %42,9 olarak kayıtlara geçmiştir. Evden İnternete erişim imkânı olmayan hanelerin %27,6'sı evden İnternete bağlanmama nedeni olarak İnternet kullanımına ihtiyaç duymadıklarını belirtmişlerdir. Yine aynı araştırmada 16-74 yaş grubundaki bireylerde bilgisayar ve İnternet kullanım oranları sırasıyla %48,7 ve %47,4'tür. Bu oranlar 2011 yılında sırasıyla %46,4 ve %45 olarak gerçekleşmiştir (Tuik, 2012). Bu istatistiki bilgilerden de anlaşılacağı üzere Türkiye'de İnternet kullanım oranları her geçen yıl artmaya devam etmektedir.

Türkiye'de gerek elektronik haberleşme altyapısının iyileştirilmesi, gerekse rekabetçi bir sektör yönünde ilerlemeler kat edilmesi için elektronik ortamı kullanan vatandaş sayısının artması ve bilgi toplumuna dönüşüm noktasında dünyada örnek olabilecek E-Devlet projelerinin hayata geçirilmesi dolayısıyla, siber güvenlik konusu ihmal edilemeyecek derecede önemli hale gelmiştir. Bilgi Teknolojileri ve İletişim Kurumu (BTK), kurulduğu 2000 yılından bu yana elektronik haberleşme sektörüne yönelik pek çok düzenleyici faaliyetin yanı sıra, sektörün güvenliğine yönelik çalışmalar da yürütmektedir. DPT koordinasyonunda yürütülen e-Dönüşüm Türkiye Projesi, Türkiye'nin bilgi toplumuna dönüşüm sürecini hızlandırmayı amaçlamakta ve bu hedefe yönelik politika ve stratejileri ortaya koymaya çalışmaktadır. Bu amaçla, "Bilgi Toplumu Stratejisi" hazırlanmış ve 2006-2010 yılları arasında atılması gereken adımları tanımlayan "Eylem Planı" oluşturulmuştur (DPT, 2011: 3). 10 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu ile birlikte BTK siber güvenlik konusundaki faaliyetlerini yoğunlaştırmıştır.

Türkiye'de siber güvenlik alanında oluşturulmuş olan ilk güvenlik politikası "Ulusal Sanal Ortam Güvenlik Politikası" Cumhurbaşkanlığı, Başbakanlık, Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Adalet Bakanlığı, Milli Savunma Bakanlığı, Maliye Bakanlığı, Ulaştırma Bakanlığı, İçişleri Bakanlığı, Devlet Planlama Teşkilatı Müsteşarlığı, Dış Ticaret Müsteşarlığı, Hazine Müsteşarlığı, Türkiye Cumhuriyet Merkez Bankası, Milli Güvenlik Kurulu Genel Sekreterliği, Milli İstihbarat

Teşkilatı Müsteşarlığı, Bankacılık Düzenleme ve Denetleme Kurumu, Emniyet Genel Müdürlüğü, Bilgi Teknolojileri ve İletişim Kurumu ve TÜBİTAK-UEKAE'nin katılımı ile Ocak 2009'da yürürlüğe girmiştir. 2013 yılı itibari ile 'Ulusal Siber Güvenlik Politikası ve Eylem Planı' TÜBİTAK Siber Güvenlik Enstitüsü tarafından Ulaştırma Bakanlığı'na sunulmuştur. Genelkurmay Başkanlığı'nın önerisi üzerine siber terör kavramı Milli Güvenlik Siyaset Belgesi'ne eklenmiştir.

Siber güvenlik faaliyetlerinin Türkiye çapında yönetilebilmesi için, Bakanlar Kurulu tarafından Ekim 2012'de imzalanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile ulusal siber güvenliğin sağlanması amacıyla Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yayımlanan plan, usul ve esaslara uyulması kararı alınmıştır. Siber güvenlik konusunda alınacak önlemleri belirlemek, hazırlanan, plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında Dışişleri Bakanlığı, İçişleri Bakanlığı, Milli Savunma Bakanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, MİT Müsteşarı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, TÜBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanı'nca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur. Ülkemizde siber güvenlik alanında faaliyet gösteren kurum ve kuruluşlar 2012 yılında artmıştır. 21 Kasım 2011 tarihinde yapılan protokolle MİT'e bağlanan eski adıyla Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanlığı yeni adıyla MİTGES olan komutanlık 15 Mayıs 2012'de alınan karar ile de Komutanlık Sinyal İstihbarat Başkanlığı'na dönüştürülmüştür. 2012 yılında TÜBİTAK BİLGEM'e bağlı Siber Güvenlik Enstitü'nün açılması sayesinde siber güvenlik alanında daha etkin ARGE yapılmasına olanak sağlanmıştır. Üniversitelerde siber güvenlik üzerine akademik çalışmaların lisansüstü ve doktora düzeyinde yürütülmesi amacı ile Yaşar Üniversitesi'nde Siber Güvenlik Bilim dalı açılmıştır. Siber güvenlik alanında faaliyet gösteren kamu kurum ve kuruluşlarının yanında sivil toplum kuruluşu olarak Bilgi Güvenliği Derneği, Siber Güvenlik Derneği, Adli Bilişim Derneği gibi kuruluşlar faaliyet göstermektedir. Ülke çapında siber güvenlik farkındalığının arttırılması,

kurumların siber saldırı anında ve sonrasında birbirleri ile koordinasyon sağlayabilmeleri amacıyla TÜBİTAK BİLGEM ve BTK tarafından düzenlenen Ulusal Siber Güvenlik Tatbikatlarının ilki 2011 yılı Ocak ayında 41 katılımcı kurum ile gerçekleştirilmiş olup, ikinci tatbikat 2013 yılı içerisinde planlanmaktadır. Siber güvenlik uzman açığının kapatılması ve üniversite öğrencilerinin siber güvenlik alanında eğitilmesinin teşvik edilmesi amacıyla, her sene, TÜBİTAK BİLGEM tarafından, "Siber Güvenlik Yaz Kampı" düzenlenmektedir (Bakır, 2012).

Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım, Bursa'da 23 Aralık 2012 yılında, siber güvenliğin ülke güvenliği ile eş değer hale geldiğini belirttiği bir konuşmada siber farkındalığa dikkat çekerek şu açıklamaları yapmıştır; "Sanal ortamda gerçek hayatın bütün işlemleri yapılıyor. Bu ve buna benzer saldırılar, bir kez daha internet güvenliğinin, siber güvenliğin ne kadar önemli olduğunu bize gösterdi. Bu saldırılar, bundan sonra da olacaktır ve bekliyoruz. Biz de gerekli tedbirleri almak için adımlarımızı attık ve planlarımızı yaptık. Vatandaşı mağdur edecek girişimlerin tedbirlerini ivedilikle almak bizim boynumuzun borcudur. Bir sosyal güvenlik kurumunun altyapısına böyle bir müdahale olduğunda milyonlarca emeklimiz, çalışanımız, doktorlarımız ve sağlık kuruşlarında işi olan vatandaşlarımız büyük bir mağduriyet yaşayabilirler. O yüzden bütün kurumlar kendi tedbirlerini almak ile beraber biz Siber Güvenlik Kurulu olarak ulusal stratejiyi belirleme ve bu ulusal siber güvenliği sağlamada da sorumlu bakanlık olarak görevimizi yapıyoruz. Tedbirler çok çeşitli. İki ana sınıfta ele almak mümkün. Birincisi altyapının korunması, yani altyapının herhangi şekilde zarar görmemesi. İkincisi ise içerdeki bilgilerin güvenliğinin sağlanması, bilgilere yapılan saldırılar sonucu sisteme yönelik işlemlerin yapılamaz hale gelmesinin önüne geçmek." olarak açıklamıştır (www.cihan.com.tr, 01.01.2014).

Türkiye'de siber güvenlik alanında NATO ile birlikte çalışmalar yürüten ve diğer kurum ve kuruluşlara göre siber güvenlik alanında üzerine nispeten daha fazla görev ve sorumluluk düşen Türk Silahlı Kuvvetleri ise kara, deniz, hava ve uzay harekât alanlarının yanında, yeni bir harekât alanı olan siber ortamda da yeteneklerini geliştirmeye başlamıştır. Bu kapsamda; siber tehditleri önleyerek, gelişmiş siber savunma ikaz ve tepki sistemlerine sahip güçlü bir merkezi siber savunma yeteneği kazanmak maksadıyla, 2012 yılında TSK Siber Savunma Merkezi Başkanlığı teşkil edilmiştir. TSK Siber Savunma Merkezi Başkanlığı siber savunma konularında

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, TÜBİTAK ve diğer kamu kurumları ile koordineli olarak faaliyetlerini icra etmektedir. Ayrıca yine bu kurum üzerinden NATO ile de faaliyetlerini ve görevlerini ulusal ve uluslararası alanda yürütmektedir. TSK'nın siber savunma güvenliğinin oluşturulması amacıyla; TSK'nın kullandığı siber ortamda bulunan tüm sistemlerin siber savunması yapılmakta, Siber olaylara anında müdahale edilmekte, Ulusal olarak ve NATO tarafından icra edilen tatbikatlara iştirak edilmekte, TSK çapında bilinçlendirme ve eğitim faaliyetleri yürütülmekte, TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetlemeleri ve testleri yapılmaktadır (www.tsk.tr, 22.01.2013).

Katılımcı kurumları siber tehditlere karşı alınması gereken önlemler ve olası saldırılar karşısında verilmesi gereken tepkiler konusunda bilgilendirmeyi ve siber güvenlik bilincinin ülke genelinde artırılmasını sağlamayı amaçlayan Ulusal Siber Güvenlik Tatbikatı, BTK ve TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) ve işbirliğiyle 25-28 Ocak 2011 tarihleri arasında, finans, elektronik haberleşme, eğitim ve savunma sektörleriyle silahlı kuvvetler, adli ve kolluk birimleri ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu ve özel sektör kurum/kuruluşunun katılımıyla gerçekleştirilmiştir (BTK, 2011).

BTK, ODTÜ, Gazi Üniversitesi ve Bilgi Güvenliği Derneği, 29 Eylül 2011'de Siber Güvenlik Çalıştayı düzenlemiştir. Çalıştayda, Türkiye'de siber güvenlik alanında bilgi birikimini arttırmak, mevcut bilgi birikimini paylaşmak ve ileride bu alanda erişilebilir açık kaynak dokümanları oluşturmak amaçlanmıştır. Çalıştay süresince, uluslararası öneme sahip olan siber güvenlik tüm boyutlarıyla ele alınmış, olası tehdit ve tehlikeler üzerinde durulup alınması gereken önlemlere ilişkin çözüm üretilmiştir (Bilişim Ajandası, 2011).

Her ne kadar Türkiye'de, siber güvenlik ve siber güvenlik algısının kurumlarda yerleşmesi adına yukarıda bahsedilen adımlar atılmış olsa da gelinen nokta halen yeterli değildir. 2023 yılına kadar en az üç nükleer enerji santrali kurma ve işletme hedefini kendisine koymuş olan Türkiye'de, İran benzeri bir siber saldırıya maruz kalmamak için atılması gereken adımlar vardır. Bunların başında siber savunma alt yapısının kurulması, siber güvenlik stratejisinin hazırlanması, savaş doktrinini siber savaşları da kapsayacak şekilde güncellemesi, bu alanda çalışacak insan gücü için istihdam açılması

ve 2012 yılında kurulan TSK Siber Savunma Merkezi Başkanlığı'nın geliştirilerek operasyonel nitelik kazanması gelmektedir (Bakır, 2012).

5. GÜNÜMÜZDE BAŞLICA SİBER SALDIRI ÖRNEKLERİ

Bu bölümde "Siber Savaş/Terörizm", "Konvansiyonel Terörizmin Değişimi", "Siber Savaşın Tanımı ve Tarihteki Gelişimi", "Siber Savaşın Hedefleri ve Amaçları (Stratejik Hedefler)" ve "Meydana Gelen Önemli Siber Saldırılar ve Etkileri" üzerinde durulmuş, örnek olaylarla siber savaş olgusunun önemine değinilmiştir.

5.1. Siber Savaş

Siber uzay, beraberinde getirmiş olduğu fayda ve fırsatlarının yanında riskleri de beraberinde getirmektedir. Siber saldırı, siber suç, siber terörizm ve son olarak siber savaşlar kavramı, siber uzayın her aşamasında etkisini artan ölçüde hissettirmektedir. Kötü niyetli amaçlar için kullanılan bu tür araçlar, başlangıçta kişisel düzeyde ya da çeşitli suç örgütleri tarafından kullanılsa da artık günümüzde devletlerinde birbirlerine karşı kullanabileceği seviyeye ulaşmıştır. 21.yüzyılın ilk 10 yılında, yaşanan olay ve saldırılar neticesinde "Siber Savaş" olgusunun dünyada ortaya çıktığı ve geleceğe yönelik derin kaygılar oluşturmaya başladığı yıllar olarak tarihe izini bırakmıştır (Alkan vd., 2012: 4).

Siber terörizm söylemi, 1990'ların başında, bilgi iletişim teknolojilerinin hızla büyümeye başladığı, "Bilgi Toplumu" kavramının sıkça tartışıldığı bir dönemde, teknoloji ve bilgisayar ağına giderek fazla bağımlı hale gelmeye başlayan ABD'nin, ileride karşılaşabileceği riskleri inceleyen çalışmaların arttığı dönemde başlamıştır. Modern araç ve gereçlerden daha da önemlisi süregelen teknolojik alışkanlıklardan mağduriyet korkusu, bilgisayar teknolojilerine olan güvensizlik ve endişe ile birleşerek toplumda siber terörizm korkusunu yaratmıştır. Amerikalı bilgisayar bilimi profesörü Dorothy Denning'e göre siber terörizm; "Siber boşluk ve terörizmin birleşimidir. Siber terörizm, siyasi ve sosyal mercilere ve kişilere gözdağı vermek, baskı oluşturmak maksadıyla resmi birimlerin bilgisayarlarına, ağ sistemlerine, bilgi ve veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır (Alnıak, 2004: 2).

ABD Federal Soruşturma Bürosu tarafından siber terörizm; "…belirgin bir politik, sosyal veya ideolojik gündeme uygun olarak, bir hükümet veya halkı etkilemek amacıyla; var olan bir kitle üzerinde karmaşa ve belirsizlik oluşturarak, korku ve dehşet yaratmak için; şiddet, yıkım ve/veya hizmetlerde aksama ile sonuçlanacak biçimde, bilgisayarların ve telekomünikasyon imkan ve kabiliyetlerinin kullanılmasıyla işlenen bir suçtur." olarak tanımlamıştır.

En temel yaklaşımla, bilgi ve bilişim ağı, bilgisayar sistemleri ile bilgisayara bağımlı sistemler üzerine yapılan saldırılara siber saldırılar denilmektedir. Siber saldırılar özel, ticari veya suç amaçlı olarak ayrılsalar dahi saldırılarda hemen hemen aynı teknik ve taktikler kullanılmaktadır. Eğer saldırı terörist amaçlı ise, siber terörizm, bilgi ve belge casusluğu yapmak amaçlı ise siber casusluk adı verilmektedir. Siber terörizm ve siber casusluğun dışında, nispeten sıradan sayılabilecek suç unsurlarına (Banka kart ve şifre bilgilerinin çalınması, hırsızlık…) ise siber suç denilmektedir (Saalbach, 2013: 6).

Teknolojik imkan ve kabiliyetlerinin insan hayatına getirdiği kolaylıklar sebebiyle artık hemen hemen bütün sistemlerde ve uygulamalarda dijital bilgiden ve onun sonuçlarından yararlanılmaktadır. Gelişmiş ülkelere ve gelişmekte olan ülkelere bakıldığında bilişim sistemi ve buna bağlı ürünler pazar payının büyük bir bölümünü oluşturmaktadır. E-Devlet uygulamaları ve bu uygulamaların kullanım alanı her geçen gün artmaktadır. Artık internet üzerinden kuruma gitmeden işlem yapabilmek, iş yerine uğramadan evde çalışmak, tüm talep ve istekleri internet üzerinden göndermek ve takip etmek çok kolay hale gelmiştir. Bu gelişme ve değişim kendisini sadece insan hayatında değil aynı zamanda mevcut diğer algı ve metotlarda da göstermektedir. Artık toplum içerisinde bireyin ve devletin rolü yeniden tanımlanmakta, hak ve özgürlükler tekrar gözden geçirilmektedir. E-Devlet sayesinde dijitalleşen devletin, mevcut uygulamaları gerçek kullanıcıya, yani ihtiyaç sahibi toplum üyesine doğru, hızlı, güvenli, eksiksiz sunma arayışı beraberinde bazı kaygıları da getirmektedir. E-Devlet uygulamaları ve bu hizmetlerin sunulması, kurum, kuruluşlar ile bireyler açısından sayısız faydaları olmasına rağmen, kritik altyapıların siber saldırılara maruz kalabileceği endişesi halen ciddi bir tehdit olarak durmaktadır. Toplum hizmetlerinin çeşitli araç ve gereçlerle sekteye uğratılması sonucu oluşturulabilecek bir karışıklık ve kargaşa ortamı, devlet otoritesini sarsabileceği gibi olası bir siber savaş ile ülke kritik altyapılarına yönelik

saldırılar, fiziki hasar ve ölümcül sonuçlar doğurabilmektedir. ABD tarafından İran Nükleer tesislerini hedef alan STUXNET siber saldırısı gibi Estonya ve Gürcistan siber savaşları bu ihtimalin hiç de uzak olmadığının bir göstergesidir. Artık düşman kuvvetlere fiziksel bir zarar vermek için savaş alanında olmaya gerek kalmamıştır, uzaktan yönlendirilebilecek siber savaşlar ve saldırılar ile çok daha fazla hasar ve zayiat verdirebilmek mümkün hale gelmiştir. Kurum, kuruluş ve devlet hizmetleri sunumundan birey ihtiyaçlarına kadar, değişen bilgi toplumu dönüşüm sürecinde artık klasik, geleneksel terörizm anlayışı da değişmektedir.

5.1.1. Konvansiyonel Terörizmin Değişimi

Teknoloji insanoğlunun hayatında her zaman bir itici güç olmuştur. Teknolojideki süregelen bu değişim ekonomi, sağlık, iletişim, spor, yönetim ve örgüt yapısı gibi birbirinden farklı alanların yanında, savaşlarda da belirleyici ve sonucu direk etkileyici bir güç olarak varlığını hissettirmiştir. Teknolojik gelişmelere tarih boyunca ya yeni bir savaş yöntemi doğurmuş ya da var olan savaş algısını değiştirmiştir. Savaşların sonucunda teknolojik gelişmeler yaşanmış ve her iki olgu da birbirinden beslene gelmiştir. Teknolojik buluş ve silahlar sayesinde klasik savaşlarda kullanılan kinetik güç yerini dijital güce bırakmaktadır. Artık adım atılmadan da dünyanın başka bir noktasına saldırılar yapılabilmekte ve hasar verilebilmektedir. İsrail Başbakanı Benjamin Netanyahu'nun siber güvenlik danışmanı Isaac Ben-Israel "Siber savaşlar konvansiyonel savaşlardaki gibi bir etki verebilecek güçtedir. Bir ülkeyi vurmak istiyorsanız o ülkenin enerji ve su kaynaklarına karşı siber ataklar düzenlemek gerekmektedir. Siber teknoloji bunu tek kurşun kullanmadan yapabilme yeteneğine sahiptir" demektedir (Bakır, 2012).

Soğuk Savaş'ın bitmesiyle birlikte gelişen ve büyüyen pazar ekonomisi, siyasi değişimleri de hızlandırdı ve şekillendirdi. Ülke savunmaları için yapılan maliyetler azalmaya başladı. Esasında yaşanan olgu değişen teknolojinin sayesinde azalan asker ihtiyacıdır. Günümüzde de devam eden bu değişim sonucunda ülkeler, geleneksel savaş metodunu terk ederek farklı saldırı veya savunma stratejilerine doğru yönelmektedirler. Günümüzde orduların sayısal büyüklükleri azalırken vuruş kabiliyetleri ve olaylara müdahale hızları artış göstermektedir. 1991 Körfez Savaşı'nın çoğu çatışma

sahnelerinin internet veya medya üzerinden canlı olarak takip edilmesi, yeni dönemin klasik savaş ve harp tekniklerinden çok daha farklı olacağının en büyük göstergesidir. Özellikle internet kullanımının sivillere de açılması ve yaygınlaşmasıyla ortaya çıkan siber uzay kavramı, asimetrik mücadeleyi teşvik eden bir alan olmuştur. İnternetin iletişimden bilgi paylaşımına kadar her alanda etkin olması, onu bir medya aracı olmaktan çıkararak, rakibe saldırılacak ve zarar verilecek bir alan haline getirmiştir (Bıçakcı, 2012: 207-209).

11 Eylül saldırılarından sonra, dünya genelinde siber terörizm tehdidi endişeleri artmış ve terörist örgütlerin daha fazla ses getirebilecek, büyük kitlesel eylemlerinde siber terörizmi araç olarak kullanılabilecekleri algısı oluşmuştur. Bilinmeyen bir gizli/sinsi tehdidin bilinen görünen tehditten daha korkutucu olduğu açıktır. Siber terörizm aslında doğrudan bir şiddet tehdidi sunmamaktadır, buna rağmen tedirgin toplumlarda yapacağı psikolojik darbe, terörist bir bombanın etkisi kadar zarar verici olabilmektedir (Alnıak, 2004: 2).

5.1.2. Siber Savaşın Tarihsel Gelişimi

Hedef olarak seçilen şahıs, şirket, kurum, örgüt gibi yapıların bilgi sistemlerine veya iletişim altyapılarına, ticari, politik veya askeri amaçlı yapılan planlı ve koordineli saldırılara 'siber saldırı', bu saldırıların ülke veya ülkelere yönelik yapılmasına ise 'siber savaş' denilmektedir (Alkan, 2014).

2007 yılında ABD Stratejik Komutanlığı daha sonradan adı siber savaş olarak değiştirilecek olan ağ savaşlarının tanımı "…hısımların kendi bilgisayar sistemlerini, bilgi sistemlerini ve ağ yapılarını etkin olarak kullanamamaları amacıyla oluşturulan bilgisayar ağ operasyonları" olarak tanımlamıştır (Saalbach, 2013: 8).

Dünyada siber algının oluşmasında aşağıda sıralanan olaylar önemli rol oynamıştır.

- 1952 yılında, dönemin Amerika Birleşik Devletleri Başkanı Sn.Truman tarafından, Amerikan karar vericilere ve askeri liderlere zamanında bilgi sağlaması amacıyla Amerikan Ulusal Güvenlik Ajansı (NSA) kurulmuştur.

1960 yılında Rusya'ya iltica eden iki NSA görevlisi ABD'nin 40 ülkenin haberleşmesini dinlediğini açıklamışlardır,

- ABD İç Savaşı sırasında General Stuart istihbarat elde edebilmek amacıyla Telgraf Hatlarını dinletmiş olması, savaş ortamında siber saldırı ve güvenliğinin önemini göstermiştir,
- (1974) William Gibson ilk kez "cyberspace" (siberalan) sözcüğünü kullanarak bu sözcüğün literatüre girmesini sağladı,
- (1992) Pentagon Bilgi Savaşları ilk "Top Secret" Yönergesi : TS – 3600 yayımlanarak yürürlüğe girdi,
- (1994) ABD Haiti operasyonunda ağ saldırılarını kullanarak, kendisine avantaj sağladı ,
- (1995) FBI'ın en çok arananlar listesine ilk kez bir hacker girdi,
- (1997) ABD Hava Kuvvetleri Bilgi Savaşları Laboratuvarı kuruldu,
- (1997) ABD'nin İlk geniş çaplı siber saldırı tatbikatı – Eligible Receiver gerçekleştirildi.
- (1998) ABD Yugoslav hava radarlarına, elektronik saldırı neticesinde sahte hedefler yerleştirdi.
- (1998) ABD Pentagondaki bir bilgisayarda tesadüfen anlaşılan veri izleme casusu programı ile Pentagon, NASA, Enerji Bakanlığı, özel üniversiteler ve araştırma laboratuvarlarındaki çok gizli evrak ve dökümanların iki yıldan uzun bir süredir izlendiğini ortaya çıkardı. Moonlight Maze adı verilen olayla ilgili yapılan inceleme neticesinde programın bağlantılarının Sovyetler Birliği ile bağlantılı olduğu anlaşılmış olsa da sonraları Rusya bu iddiaları reddetti.
- (2000) Alman İçişleri Bakanlığı, Nazi sitelerine karşı DDOS (denial of service attack-Servislerin hizmet veremez hale getirilmesi) saldırıları gerçekleştirebileceklerini söyledi. Alınan tepki üzerine bu demeç geri çekilmek zorunda kaldı.
- (2001) AB, ABD'nin baskılarına rağmen GPS'e rakip olarak gösterilen ve hemen hemen aynı frekans aralığını kullanan Galileo GPS sistemini finanse etme kararı aldı (Sağıroğlu, 2013: 45).

5.1.3. Siber Savaşın Hedefleri ve Amaçları (Stratejik Hedefler)

Terörist örgütler açısından değerlendirildiğinde, siber terörizm, en basit yöntemle, ağa bağlantılı kişisel bilgisayar ile yapılabileceğinden dolayı, geleneksel anlamdaki terör metotlarından daha az maliyetlidir. Siber saldırıda, saldırı yapan kişiler, kendi kimliklerini, diğer saldırı yöntemlerine nazaran daha iyi gizleyebilmektedirler. Dolayısıyla siber boşlukta saldırganları durdurabilecek fiziki bariyerler, kontrol noktaları gibi engeller bulunmamaktadır. Siber saldırının yönlendirilebileceği kamu kurum ve kuruluşlarının yanında kritik hizmetleri yöneten özel kuruluşlar gibi saldırı yapılabilecek noktaların çokluğu dolayısı ile bu kadar çok hedef arasında zayıf ve savunmasız bir nokta bulma olasılığı fazladır (Alnıak, 2004: 5-6).

Tablo 5: AB ve ABD Tarafından Belirlenmiş Olan Kritik Altyapılar

AB	ABD
Su Gıda Sağlık Enerji Finans Ulaşım Sivil Yönetim Bilgi ve İletişim Uzay ve Araştırmaları Kimyasal ve Nükleer Endüstri Kamu Düzeni ve Güvenlik Alanı	Su Enerji Ulaşım Tarım ve Gıda Kolluk Hizmetleri Bilgi ve İletişim Bankacılık ve Finans Bayındırlık Hizmetleri Federal ve Yerel Hizmetler Acil Hizmetler (sağlık, itfaiye, vb.)

Kaynak: Brunner, E., ve M. Suter (2009: 433-483).

Siber savaşın belli başlı amaçlarını; Casusluk, bilgi kirliliği, bilgilerin manipülasyonu (değiştirme, silme, ifşa etme, çalınması), siteme yetkisiz erişim, propaganda, dolandırıcılık, iletişimin kesilmesi, siber bombalarla sabotaj, sistemin

bozulması ile birlikte halk arasında kaos yaratma olarak tanımlayabiliriz (Sağıroğlu, 2013: 63).

Zarar görmesi veya yok olması halinde, vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik refahına veya hükümetin etkin ve verimli işleyişine ciddi olumsuz etki edecek, fiziki ve bilgi teknolojileri tesisleri, şebekeler, hizmetler ve varlıklar AB Komisyonu tarafından kritik alt yapılar olarak belirlenmiştir. Tablo 5'te AB ve ABD tarafından belirlenmiş olan kritik altyapılar listelenmiştir. Bu kritik alt yapılar bir ülkenin, siber güvenliğinin sağlanabilmesi için son derece önemlidir. Siber güvenlik ve caydırıcılığın asıl hedefi, kritik alt yapıları korumaktır. Klasik savaşta öncelikli hedef olarak değerlendirilen bu sistem veya yapılar, siber savaşta da birinci hedeftir. Siber savaşın asıl amacı olası kriz veya savaş öncesi durumlarda psikolojik ve durumsal üstünlüğü sağlayarak, sonrasında icra edilecek harekâta kolaylık sağlamaktır. Siber savaş tek başına kritik alt yapıları etkileme kabiliyetine sahip olsa da, yaratacağı hizmet kesintisi sınırlı ve dönemsel olacaktır. Dünya genelinde yaşanan büyük deprem, sel veya diğer doğal afetler göstermiştir ki, kritik alt yapılar felaketten çok kısa bir süre sonra hizmet verebilir hale getirile bilinmektedir (Lewis, 2006: 1-4).

5.2. Başlıca Siber Saldırı Örnekleri

İnternetin ve bilişim teknolojilerin insanoğlunu hayatına girmeye başladığı 90'lı yıllarda, Rus birlikleri Rusya'nın toprak bütünlüğünü sağlamak amacıyla Aralık 1994'te Çeçenistan'ın başkenti Grozni'ye girdi. Görece olarak donanımlı silah ve teçhizata sahip olan Rus birlikleri Çeçen direnişinin kısa süreceği zannediyordu. Ancak savaş alanındaki gerçekler beklentileri karşılamadı. Soğuk savaş sonrasında, silahlı çatışma ilk defa internet ortamına taşındı. Çeçenler başta internet olmak üzere bütün medya kanallarını kullanarak, bilgi savaşının ilk örneklerini verdi. Çeçenlerin internete yükledikleri ölü Rus askerlerin resimlerini gören anneler, çocuklarını kurtarmak için harekete geçtiler. Ruslar geleneksel savaşın dışında oluşan bu siber alanın etkisini anlamakta gecikmiş olsalar da bir süre sonra siber ortamda yapılan bu saldırılara karşı başka siteler açarak cevap verdiler. Siber alanda gerçekleşen ilk soğuk mücadele günümüzde gerçekleşen siber savaşların öncülüğünü yaptı. Genellikle siber saldırıya uğrayan kurum veya kuruluşlar itibarlarını korumak amacıyla yapılan saldırıları

gizlemeyi tercih etseler de bilinen belli başlı siber savaş/saldırılara aşağıda değinilmiştir (Bıçakcı, 2012: 209-222).

5.2.1. Estonya 2007 ve Gürcistan 2008 Siber Savaşları

> İnternet kullanımının yüksek düzeyde olduğu ülkelerden birisi olan Estonya, vatandaşlarının devlet kurumlarına ve bankalarına internet üzerinden bağlanmasına imkân veren bir dijital kimliğe sahiptir. Ülkede 355 devlet kuruluşu hizmetlerini internet üzerinden yürütmektedir (Ernsdorff ve Berbec, 2007: 171'den aktaran Bıçakcı, 2012: 214).

Estonya'nın E-Devlet yapılanmasında Orta ve Doğu Avrupa'da lider ve dünyada üçüncü sırada yer aldığını belirtilmektedir. Yine Estonya, 2005 yılında dünya üzerinde ilk defa internet üzerinden yapılmış olan yerel seçimlere de ev sahipliği yapmıştır (Gelinas, 2010: 7). 2010 yılı verilerine göre, Estonya'nın nüfusun yüzde 75'e yakını internet kullanıcısıdır. 2002 NATO Prag Zirvesi sonrası, üyelik görüşmelerine başlayan Estonya 2003'te NATO'ya üye olarak kabul edilmesiyle Rusya'dan politik anlamda uzaklaşmaya başlamıştır (Bıçakcı, 2012: 214-217). İkinci Dünya Savaşı sırasında Estonya, Sovyetler Birliği ile beraber, Almanya'ya karşı savaşmıştır. İkinci Dünya Savaşı sona erince Estonya'nın başkenti Tallinn'e Kızıl Ordu'nun girişini simgeleyen Bronz Asker Anıtı 1947 yılında dikilmiş ve bu heykelin 26 Nisan 2007'de yerinden kaldırılmasından bir gün sonra, heykelin kaldırılması Rusya Federasyonu tarafından kınanmıştır. Daha sonrasında ise ülke içerisinde ayaklanmalar baş göstermiş ve bu protestolar sanal saldırılara dönüşmüştür (Bakır, 2012).

Ülkenin siber altyapısını hedef alan saldırılar 27 Nisan gecesinde başladı. Sunulan hizmetlerin yoğunluktan dolayı hizmet verememesi (DoS) şeklinde gerçekleştirilen saldırı, Rus internet sitelerinde, teknik bilgisi olmayan sıradan bilgisayar kullanıcılarına, saldırıların nasıl ve hangi sitelere yapılacağının gösterilmesi suretiyle yaygınlaştırıldı. Saldırı süresinde nispeten siber saldırılara karşı önlem alabilmiş olan birkaç banka dışında saldırıya hazırlıksız yakalanan devlet siteleri hizmet veremez hale geldi. Yapılan bu koordine saldırılar 23 Mayıs'a kadar devam etti. Saldırganların IP izlerinin ABD, Kanada, Rusya, Türkiye, Almanya, Belçika, Mısır ve Vietnam gibi ülkelerden yapıldığı görüldüğünde düşmanın ve saldırganın kim olduğu açık olarak anlaşılamamıştır. Saldırılar sonrası Estonya Savunma Bakanı Dr. Jaak Aaviksoo'nun NATO'dan yardım

çağrısı sonucunda NATO da olaylara hızlı ve etkili bir şekilde müdahil olmuştur (Bıçakcı, 2012: 214-217).

Dünya literatöründe her ne kadar bağımsız gibi görünse de hala büyük oranda Rusya'ya bağımlı olan Estonya ve Gürcistan, Rusya için siber saldırı testi açısından mükemmel iki deneme sahası olmuştur. Rusya bu iki ülkeye yaptığı saldırılarla ülkede bulunan resmi kuruluşların, finans ve basın-yayının bütün iletişimini 3 hafta süreyle kesintiye uğratmıştır. Bu iki olay üzerine NATO 2008 yılında Estonya'nın Tallinn şehrinde bir siber savunma merkezi kurdu. ABD Savunma Bakanlığı ülkelerin füze sistemlerine, enerji boru hatlarına, basın yayın merkezlerine yapılan siber saldırıları savaş sebebi sayacağını açıkladı ve kritik alt yapıları kullanamaz hale getirmeye yönelik her türlü siber saldırıya klasik savaş unsurlarıyla karşılık vereceğini belirtti (Alkan, 2014).

Estonya siber savaşının üzerinden bir yıl geçmeden Rus Federasyonu ile Gürcistan, Güney Osetya sebebiyle karşı karşıya geldi. 7 Ağustos 2008 yılında Gürcistan Güney Osetya'ya toprak bütünlüğünü sağlamak amacıyla operasyon başlattı. Buna karşılık da Rus birlikleri 8 Ağustos'ta Osetya'ya girerek Gürcistan'ı işgal etti. Rusya'nın Gürcistan'a karşı saldırısı aslında siber olarak 7 Ağustos 2008 akşamında başlamıştı. Gürcistan Estonya kadar E-Devlet sistemleri üzerinde internete bağımlı olmaması sebebiyle fazla etkilenmemiş olsa da Gürcistan'ın NATO'ya üyeliği henüz gerçekleşmemiş olması dolayısıyla, Gürcistan NATO'nun güvenlik şemsiyesinden faydalanamamıştır. Gürcistan'a karşı yapılan bu siber saldırı, geleneksel savaş yöntemleriyle beraber kullanılması bakımından gerçek bir hibrit savaş olarak tanımlanabilir (Bıçakcı, 2012: 217-219).

5.2.2. ABD-İran Siber Savaşı: Stuxnet

ABD, Rusya'nın Estonya ve Gürcistan Siber saldırılarına karşılık olarak İran Siber Saldırısını gerçekleştirdi. Rusya için ortadoğuda büyük önem taşıyan bir ülke olan İran'a saldırı ABD ve İsrail'in karşı çıktığı İran'ın nükleer programını engellemek veya sekteye uğratma amacını taşıyordu. Ortadoğu politikalarında ve nükleer programının geliştirilmesi süresince, Rusya'nın desteğini alan İran'a, ABD tarafından gerçekleştirilen siber saldırı oldukça özgün ve ezber bozan bir taktik içeriyordu. Kendi

kendini kopyalayan bir yazılım olan Stuxnet virüsü ile ABD öncelikle motorları ve sıcaklığı kontrol eden merkezi mantık kontrol birimi olan PLC'yi ele geçirdi. Böylece sistemi kontrol eden diğer yazılımlar da kolaylıkla elemine edebildi. Sonuç olarak özellikle nükleer yakıt zenginleştirme tesislerini hedef alan bu saldırı santrifüjlerin olması gerekenden daha hızlı bir şekilde dönmesine yol açtı ve etkilediği sistemlere ciddi fiziki zararlar verdi. İran saldırının başında ne olduğunu tam olarak kavrayamasa da daha sonraları durumun vahametini anladı ve en yetkili ağızdan bizzat İran Cumhurbaşkanı Ahmedinejad tarafından İran'ın bir siber saldırıya uğradığı doğrulandı. Stuxnet'i özel kılan en önemli şey sadece internete bağlı bilgisayarları değil her hangi bir veri girişi yapılan (USB, CD, Harici Bellek vb. aracılığıyla) bilgisayarı da ele geçirebilmesi ve kendine yönelik kullanabilmesiydi. İran'da bu saldırı sonucu tam 62.867 bilgisayara stuxnet solucanı bulaştığı tahmin edilmektedir (Alkan, 2014).

Yapılan bu siber saldırı neticesinde 2010 yılında, İran'ın tüm santrifüj sayısının 1/5'ine denk gelen 1000 santrifüj donanımsal olarak çalışamaz hale getirilmiştir. Stuxnet zararlı yazılımının dünya üzerinde 130.000 bilgisayarı etkilediği ve bu bilgisayarların %60'ının İran'da bulunduğu tahmin edilmektedir (Bakır, 2012).

Bu saldırı siber savaş ve siber güvenlik algısının ne kadar önemli olduğunu, sistemlerin internet gibi erişime açık ağlar olmasa dahi saldırıya maruz kalabileceğini, çok basit yazılımlarla önemli ve stratejik alt yapılara kolaylıkla saldırı yapılabileceğini göstermesi açısından önemlidir.

5.2.3. Wikileaks

Yakın tarihimizde yaşanan ve tarihe wikileaks belgeleri olarak geçen olaylar neticesinde, ABD Büyükelçilikleri tarafından gönderilen yaklaşık 250.000 gizli diplomatik belge internet sitesi üzerinden yayımlanmıştır. 28 Aralık 1966 tarihinden 28 Şubat 2010 tarihine kadar olan diplomatik yazışmaları içeren belgeler arasında ABD'ye ait 15.652 belge "gizli" olarak nitelendirilmektedir. 15.365 belge ile Irak, belgelerde en çok adı geçen ülkedir. Irak kaynaklı belgelerin sayısı 6.677'dir. ABD Dışişleri Bakanlığı'ndan 8.017 belge gelmiştir. Türkiye'nin ise 7.918 belgeye kaynaklık ettiği bilinmektedir. ABD Dışişleri Bakanlığı'nın etiketleme sistemine göre belgelerin 145.451'i dış siyasi ilişkilerle, 122.896'sı hükümetlerin kendi iç meseleleriyle, 55.211'i

insan haklarıyla, 49.044'ü ekonomik koşullarla, 28.801'i teröristler ve terörizmle ve 6.532'si BM Güvenlik Konseyi ile ilgilidir (Turgut, 2011: 9). Wikileaks oluşumu, ABD başta olmak üzere devletlerin gizli politikalarını dünya kamuoyu ile paylaşmayı amaçlamıştır. İnternet sitesinde kendisini kar amacı gütmeyen bir medya kuruluşu olarak tanımlamakta, asıl amacının önemli haber ve bilgileri kamuoyuna iletmek olduğunu belirtmektedir. Dünya üzerinde 274 farklı ABD Büyükelçiliği tarafından gönderilmiş belgelerinden oluşan bu bildirimlerde, düşman ülke tanımlarından ülke önderleri hakkındaki analizlere, Birleşmiş Milletler liderleri hakkında casusluk isteğinden kritik altyapı açıklıklarına kadar geniş bir perspektifteki gizli bilgiler açığa çıkmıştır. İlk yazışmaların site üzerinden yayımlanmasıyla birlikte, siteye karşı siber saldırının olduğu WikiLeaks Grubunun kurucusu olan Julian ASSANGE tarafından belirtilmiştir. Sonraları grubun mevcut özel sektör şirketleriyle olan ilişkileri birer birer kesilmiştir. Önce Amazon.com internet sağlayıcısı WikiLeaks internet sitesini sunucularından kaldırmış, sonra gruba yapılan yardımlarının toplandığı PayPal hesabı kapatılmış, Mastercard ve Visa gibi şirketler grup hesaplarından ödeme almayı durdurmuşlardır. Bu yaptırım sayılabilecek adımlara cevap olarak Anonymous korsan gurubu, hizmet durduran şirket ve gruplara karşı siber saldırılarda bulunmuştur. Bu olay, siber uzayda, iki farklı korsan grubunun gerekirse kolaylıkla güçlerini birleştirerek bir birlerine yardım edebileceklerini göstermiştir (Pras vd., 2010).

WikiLeaks grubuyla doğrudan veya dolaylı olarak parasal ilişki içerisinde olan firmaların birer birer grupla olan bağlantılarını koparmaları sonucu, Ekim 2011 yılında grubun kurucusu Julian ASSANGE, yapılan finansal ambargolar sebebiyle gelirlerinin %95'ini kaybettiklerini ve artık belge yayımlamayı durdurduklarını açıklamıştır (http://en.wikipedia.org, 23.03.2013).

Yayımlanan bu belgeler, devletlerin ulusal ve uluslararası gündemini uzun bir süre meşgul etmiştir. Giderek kamuoyundaki etkisi azalsa da yayımlanan her yeni belge, dünya siyasetinde etkisini hissettirmiştir. Wikileaks belgelerinin internet ortamından yayımlanmasıyla birlikte, farklı tartışmalar meydana gelmiştir. Bir yandan hızla gelişen iletişim teknolojilerinin, devletlerin ve kişilerin gizli bilgilerini açığa çıkarmaması gerektiğini savunanlar ile bireylerin, devlet politikaları hakkında bilgi sahibi olmaları gerektiğini savunanlar olmuştur. Belgelerin doğruluğu bizzat ABD tarafından doğrulanmıştır. Wikileaks belgeleri henüz yayımlanmadan önce, olası etkileri en aza

indirebilmek amacıyla ABD hükümeti, belgelerde adı geçmesi muhtemel ülkeleri önceden bilgilendirmiştir (Turgut, 2011: 8-10).

Belgelerin elde edilmesinde, ABD Arizona eyaletinde bir dönem askeri istihbarat analiz elemanı olarak eğitim almış olan kıdemli onbaşı Bradley MANNING'in rolü olduğuna inanılmaktadır. Adı geçen şahıs tutuklu olarak halen ABD Virginia askeri üssünde alı konulmakta ve askeri mahkemede yargılanmasına başlanacaktır (The New York Times 07.09.2014). WikiLeaks ve onun sebep olduğu gizli dosyaların ifşaa edilmesi olayı küçük bir grup ya da kuruluşlarla, bir ülkenin ulusal veya uluslararası saygınlığına, etkinliğine ve güvenliğine derin ve sarsıcı bir hasar bırakabileceğinin bir göstergesidir (Sterner, 2011). Wikileaks olayı siber güvenlik açısından incelendiğinde, gizli bilgi ve belge sızdırılmasında en zayıf halkanın şirket, kurum veya devlet çalışanlarından birisi, yani insan olduğu bir kez daha görülmüştür. Rütbe olarak alt seviyelerde olan bir çalışanın dahi, gizli bilgi ve belgelere bu kadar kolay nüfus ederek, sistemden kopyalayabilmesi halen ABD Savunma Bakanlığı'nda sorgulanmaktadır. Siber güvenliğin sağlanmasında ve muhafazasında insan faktörü kilit önem taşısa da sisteme olan erişimin yetkilendirilmesi ve sistem üzerindeki işlemlerin kısıtlanması büyük önem taşımaktadır. Sistem üzerinde gerekli güvenlik önlemlerinin (dosya indirememe, kopyalayamama, değiştirememe gibi…) alınmasının siber güvenliğe katkı sağlayacağı değerlendirilmektedir.

5.2.4. Operasyon Moonlight Maze 1998-2000

Dünyada henüz siber savaş algısı oluşmamışken, Rusya tarafından yapıldığı tahmin edilen, ABD tarihindeki ilk siber saldırı kabul edilebilecek "Moonlight Maze" olayı yaşanmıştır. Mart 1998 de ABD Savunma Departmanı çalışanları tarafından kazara fark edilen bir casus yazılım sayesinde, iki yılı aşkın bir süredir, Pentagon, NASA, Enerji Departmanlığı, Özel Üniversiteler ve Araştırma Laboratuvarları hakkında bilgi sızdırdığı öğrenilmiştir. Yapılan araştırmalar sonucunda gelen ve giden veri paketlerinin Rusya'da konuşlu sunucular üzerinden olduğu tespit edilmiş olmasına rağmen Rusya bu konu ile ilgisi olmadığını belirtmiştir. Operasyon Moonlight Maze ile birlikte, ABD siber güvenlik algısı ile karşılaşmış ve bu yeni algı karşısında alınması gereken adımları almaya hızla başlamıştır (Gelinas, 2010: 10-11). Casus yazılımın elde

ettiği bilgiler içerisinde kişi ve çalışan personellerin iletişim bilgileri, askeri bölge haritaları, birlik kuruluşları ve askeri donanım tasarımları bulunmaktaydı (http://en.wikipedia.org, 23.03.2013).

5.2.5. LulzSec (ABD Senatosu)

Yüksek seviyede güvenlik sistemlerine sahip olan sistem ve kurumlara yaptığı saldırılarla ismini duyuran Lulz Security korsan grubu, ABD Merkezi Haber Alma Teşkilatı'nın internet sitesi başta olmak üzere, İngiliz Ulusal Sağlık Servisi, Portekiz Bankası, Sony, Nintendo gibi kurumlara siber saldırılarda bulunmuştur. 13 Haziran 2012 tarihinde grup, bazı ABD Senato üyelerinin kullanıcı adı ve şifrelerini kırarak yayımlamıştır. Grup her ne kadar senato üyelerinin kullanıcı adı ve şifrelerini ele geçirmiş olsa da, gizli bilgi ve belgeleri elde edememiştir. Daha sonra ABD Senatosundan yapılan açıklamada, kullanılan ateş duvarı(firewall) sayesinde grubun gizli bilgi ve belgelere erişemediği belirtilmiştir. ABD Senato saldırısı, gerekli güvenlik tedbirlerinin yerinde ve zamanında etkin araçlarla alınması durumunda güvenlik zafiyeti yaşanmadan atlatılabileceğini göstermesi bakımından önemlidir (http://en.wikipedia.org, 23.03.2013).

5.2.6. Türkiye'de Meydan Gelmiş Olan Siber Saldırılar

Meydana gelen siber saldırıların, halkın nezdinde, kurum veya şirket görünümünü kötü yönde etkileyeceği, marka değerine zarar vereceği, E-Devletleşme yolunda atılan adımları ve yapılan çalışmaları etkileyebileceği, saldırıya uğrayan ve zarar gören sistem, kurum ve kuruluşlara yönelik güven bunalımı yaşanabileceği kaygıları nedeniyle, yapılan bu saldırılar resmi olarak kabul edilmemekte ve verilen zararların boyutları tam olarak bilinememektedir. Ülkemizde de yapılan bu saldırılar kimi zaman basılı ve yazılı medyada yer edinmiş olsa da resmi olarak saldırının boyutları tam olarak öğrenilememiştir. Dünyada en çok siber saldırıya uğrayan 10 ülkeden biri olan Türkiye'de (www.boydakbilisim.com 27.11.2014) yazılı ve görsel medyada çıkan, siber saldırılardan bazıları şunlardır;

2001 yılında, Türkiye'de yapılan siber casusluk faaliyeti sonucu, yabancı gizli servisler, kamu bankalarının yazılımını karşılamak için kurulan Finansal Teknoloji Hizmetleri A.Ş şirketi üzerinden, bu şirketin yazılım hizmeti sağladığı Ziraat ve Halk Bankası'nda saklanan tüm verileri ve kamu bankalarına ait bir çok bilgiyi ele geçirmeyi başarmışlardır. Aksiyon dergisinin haberine göre, ABD Merkezi Haber Alma Örgütü(CIA) ve İsrail gizli servisi (MOSSAD) tarafından ortaklaşa gerçekleştirilen bu operasyonla maaşını kamu bankalarından alan 5.000 (beş bin) MİT mensubunun da gerçek kimliği açığa çıkmış ve bu siber saldırı sonucunda, MİT adına çalışan isimlerin gizliliği kalmamıştır (http://beta.yenisafak.com.tr 20.05.2014).

İnternetin bilinen korsan gruplarından biri olan Anonymous, Bilgi Teknolojileri ve İletişim Kurumu'na saldırıda bulunmuş saldırı sonucu elde ettiği tüm bilgileri internette yayınlanmıştır. Grubun elde ettiği veriler arasında, BTK çalışanlarının kullanıcı isimleri, e-posta adresleri, kriptolu halde şifreleri, BTK'nın sistemlerine uzaktan erişen firmaların sisteme giriş isimleri ve kriptolu halde şifreleri bulunmuştur. Bu firmalar arasında Vodafone, TTNet, Superonline, Avea, Türkcell gibi önde gelen büyük teknoloji şirketleri bulunmaktadır (www.sabah.com.tr 14.02.2012).

MERNİS sistemi üzerinden temin edildiği anlaşılan, yaklaşık 70 milyon kişinin kimlik, adres ve telefon bilgilerini yasa dışı yollarla elde ettikten sonra bazı hukuk bürolarına sattığı anlaşılan suç örgütü çökertilmiştir (Örnekoğlu, Milliyet 28.07.2010).

Milli Eğitim Bakanlığı'nın 687 bin öğretmene ait kayıtların tutulduğu İl ve İlçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi'nin (İLSİS) korsanların saldırısına uğramıştır. Öğretmenlerin isim, soy isim, T.C. kimlik no ve okul isimlerinin bulunduğu bilgileri dosya paylaşım sitesinde paylaşıma açıldı. MEB, bakanlık çalışanlarında bir güvenlik zafiyeti olup olmadığı ile ilgili soruşturma başlattı. MEB saldırganların İLSİS'in yalnızca bir ateş duvarını aşabildiğini, 12 ateş duvarını aşamadıklarını açıkladı (Bulut, Yeni Şafak 13.02.2014).

Redhack korsan gurubu tarafından yapılan, YÖK'ün elektronik belge yönetim sistemine yönelik siber saldırısı sonucu, sistemin veri tabanında bulunan ve gizlilik değeri taşıyan bazı bilgi ve belgeler, grup tarafından ele geçirilmiştir. YÖK'ten yapılan yazılı açıklamada, kurulun iş süreçlerini hızlandırmak amacıyla geçen ay hayata geçirdiği elektronik belge yönetim sisteminin, 8 Ocak 2013 tarihinde siber saldırıya uğradığı ve veri tabanında yer alan, gizlilik taşıyan bazı bilgi ve belgelere hukuk dışı

yollarla ulaşılarak paylaşılmasına ilişkin suç duyurusunda bulunduğu açıklanmıştır (www.radikal.com.tr 10.01.2013).

6. SİBER ÜLKE GÜVENLİĞİ KAYGILARININ E-DEVLETLEŞME SÜRECİNE ETKİSİ VE ALINMASI GEREKEN TEDBİRLER

6.1. Siber Ülke Güvenliği Kaygısı

Önceleri kişisel bilgi ve belgeleri ele geçirerek maddi kazanç sağlamaya yönelik saldırılar ile başlayan, siber saldırılar, sonrasında siber uzayın saldırganlara sağlamış olduğu zor tespit edilebilme veya tespit edilememe avantajları sayesinde boyut değiştirerek kamu yönetimini ve devlet güvenliğini etkiler boyutlara ulaşmıştır. E-Devletleşme sürecinde, kurumlar ve birimler arası yazışmaların elektronik ortamda yapılmasını sağlayan, belge ve bilgi yönetim uygulamasının, yetkisiz kişi ve kurumların eline geçmesi sonucu bir ülkenin içine düştüğü durumu bize wikileaks olayı göstermiştir (Turgut, 2011: 8-10). Ülke itibarının sarsılması, psikolojik üstünlük elde etme ve mevcut ilişkilerin tekrar okunması ve tanımlanması açısından basit argumanlarla yapılan siber saldırıların sonuçları sadece siber uzayda değil gerçek dünyada da kendisini hissettirmektedir. Bundan 10-15 yıl öncesine kadar bireysel ve devlet yönetimi anlamında aşina olunmayan, genelde bilim kurgu sahnelerinde görülen ve öyle kalacağı tahmin edilen siber saldırı ve savaşlar, Estonya'ya ve İran'a yapılan kritik saldırılarla ne kadar gerçek ve hasar yaratıcı etkiye sahip olduğunu göstermiştir (BTK, 2013).

6.2. Siber Ülke Güvenliği - Kamu Yönetimi İlişkisi

Küreselleşmeye ayak uydurmak zorunda olan insanoğlu, devlet yönetiminde de ona ayak uydurmak zorundadır. Bilişim teknolojileri ile hizmet kalitesini arttıran yeni devlet yönetimi anlayışı, bu yeni düzene karşı yapılan saldırıları da önleme adına adım atması gerekmektedir. Aksi halde, hizmetlerini yeni düzenin sağladığı bilişim kanalları

vasıtasıyla alan toplumda büyük bir kargaşa meydana gelir. Siber güvenliğin sağlanmasında geç kalınması, e-devlet ve uygulamalarının verimli çalışmamasına, bu da topluma kamu yönetimleri açısından kaliteli hizmetin sunulamamasına sebep olur. Sistemlerin her geçen gün elektronik ortamdan yürütülmeye başlandığı bu yeni bilişim toplumunda güvenlikte artık sanallaşmıştır. Gizli bilgi ve belgelerinde tutulduğu bu bilişim ortamında meydana gelebilecek bir saldırı durumunda ülke güvenliğini etkileyici büyük kayıpların olabileceği artık bir gerçektir. Kamu kurum ve kuruluşları, siber güvenliği sağlama adına atılması gereken adımları devlet öncülüğünde yapmalı ve sistemi olası tüm saldırılara karşı korunaklı hale getirmelidir. Aksi halde Türkiye'de yaşanan Milli İstihbarat Teşkilatı'nın personel ve muhbir bilgilerinin istenmeyen kişilerin eline geçmesi gibi kamu kurumunun çalışmasını derinden sarsabilecek olaylarla karşılaşılabilinir (http://beta.yenisafak.com.tr 20.05.2014).

Siber ülke güvenliği kamu yönetimi ile yakından ilişkilidir. Kamu kurum ve kuruluşlarının yürütmüş olduğu hemen hemen tüm elektronik faaliyetler siber saldırılara maruz kalabilecek durumdadır. Yönetimi klasik devlet anlayışına göre çok daha kolay olan e-devlet sistemlerinin hizmete sunulmasından sonra klasik yöntem kamu kurumları tarafından kullanılmadığı için ya unutulmakta ya da güncelliğini yitirmektedir. Olası bir siber saldırı durumunda eğer kamu kurum veya kuruluşu gerekli tedbirleri almamış ise, e-devlet uygulaması yerine klasik devlet uygulamalarını (kağıt, dosya, evrak) tekrar tesis etmekte zorlanmakta ve bu da hizmetin tekrar sunulmasını geciktirmektedir. E-devlet uygulamalarının yerine tekrar klasik devlet anlayışına göre hizmeti devreye almak hem külfetli ve zaman alıcı hem de güncelliğini yitirmiş olduğundan dolayı e-devlet uygulamasının yerine tam manasıyla geçememektedir.

Günümüzde, küreselleşmenin etkisi ve teknolojinin yardımıyla, toplumların bilgi toplumuna dönüşüm süreci hızlı bir şekilde devam etmektedir. Bireylerin, kurumların ve ülkelerin İnternet başta olmak üzere bilgi iletişim teknolojileri ve bu teknolojilerin getirmiş olduğu yeni kullanım alanlarına olan bağımlılığı giderek artmaktadır. Bilgi toplumu içerisinde kendisine çokça yer edinen bilgi teknolojileri, artık hayatı desteklemekten de öte hayatın kendisi olmuştur. Bu gelişmeler rağmen, hayatımızın artık ayrılmaz bir parçası haline gelen İnternetin sınır tanımayan küresel yapısı ve beraberinde getirdiği küresel ilişkiler sebebiyle pek çok güvenlik açığı oluşmakta ve bu açıkla siber ülke güvenliğini tehlikeye sokmaktadır. Başta ufak kredi kartı veya bireysel

bilgilerin çalınmasıyla başlayan siber saldırı ve savaş süresi, devamında ülke servis ve hizmetlerinin devre dışı bırakılmasını amaçlayan karışık bir yapıya bürünmüştür. Ülkede kargaşa ortamı yaratmaya dair hedefleri olan hasım birçok yasal veya yasal olmaya gurup ve ülkeler bu alanda etkin olabilmenin çabası içerisine girmişlerdir. Bir ülke kurum ve kuruluşlarının, vermiş olduğu hizmetler ne kadar dijitalleşmiş ise, yani bir ülke ne kadar E-Devletleşme sürecinde ilerlemiş ise, o ülkenin siber saldırılara maruz kalma riski de o derecede artmış demektir (Alnıak, 2004: 2).

2000'li yıllarda yaşanan siber saldırılar ve siber savaşlar nedeniyle, yöneticilerin dikkatini çeken siber güvenliği sağlayabilme kaygısının, bilgi toplumu dönüşümü süreci önündeki bir engel olduğu değerlendirilmektedir. Her ne kadar siber ülke güvenliği kaygısı, E-Devletleşme süreci üzerinde bir baskı unsuru olarak bulunsa da teknolojinin insanoğluna sunduğu yeni imkan ve kabiliyetlerden vazgeçmek veya geri kalmak mümkün görünmemektedir. E-Devletleşme sürecinde, kamu kurumlarının genel olarak dağıtımını ve hizmet sunumunu üstlendiği kritik hizmet kollarına, teknoloji kullanılarak yapılan siber saldırılar, yine teknoloji kullanılarak önlenebilmektedir. Herhangi bir siber saldırı sonrası, etkilenen servis veya hizmetlerin yerine geçebilecek ikinci bir çözüm, günümüz küresel dünyasında özel sektörün katkısıyla veya oluşagelmiş uluslararası kuruluşların dinamik yapısı sayesinde korku olmaktan çıkmaktadır. Yaşanabilecek siber saldırıların, gerekli önlem ve tedbirler zamanında ve bilinçli bir şekilde alındığı takdirde etkisinin kısıtlı olacağı değerlendirilmektedir. E-Devletleşme sürecinde sistem içerisinde kullanılan uygulama ve yazılımların yekpare bir yapıda olmadığından, siber savaşlarda etkilenen bölüm kolaylıkla devre dışı bırakılabilir ve sitemin genel hatlarıyla çalışması sağlanabilir. Yine bu sistemlerin hemen hemen çoğunda sistemin genelinden ziyade bir kısmı kritik öneme sahiptir. Bu kritik kısım ve bölümlerin korunaklı olması durumunda siber saldırıların etkileri, ulusal güvenliği etkileyici boyutlarda olmayacaktır. Yapılan çalışmalar göstermiştir ki, eski ve kendisini güncellememiş olan sistemler siber saldırılardan çok daha fazla etkilenmektedir (Kenyon, 2009). Siber güvenlik kaygısı ile teknolojik gelişmelerin takip edilmemesi durumunda, yaşanacak olası bir siber saldırının ülke güvenliğine yaşatacağı etki daha büyük olacaktır. E-Devlet uygulamalarının getirileri ve kazançlarının yanında, siber ülke güvenliği kaygısı kabul edilebilir bir risk olarak durmaktadır (Lewis, 2006: 2-7). E-Devletleşme sürecinde siber ülke güvenliğinin sağlanması amacıyla, en altta bulunan kullanıcı veya vatandaştan en

üste kadar bir takım sorumluluklar ve görevler düşmektedir. Siber güvenlik tek başına bir kurum veya kuruluşun sorumluluğunda sağlanabilecek bir olgu değildir. Devlet yönetiminin, kamu kurum ve kuruluşlarının, özel sektör firmalarının ve kullanıcıların bir arada çalışması ve üzerine düşen görevleri yerine getirmeleri gerekmektedir (Government of Canada, 2010: 9-13).

6.3. Siber Ülke Güvenliğinin Sağlanması Amacıyla Alınması Gereken Tedbirler

Uluslararası sistemde, hukukla kayıt altına alınan casusluk, teknik hırsızlık, bilgisayar korsanlığı, servisin hizmet veremez hale getirilmesi gibi fiiller siber ortamda, hiç bir kısıtlama olmadan gerçekleştirilebilmektedir. Siber saldırganların, çeşitli yöntemler kullanarak, saldırılarının kaynağını gizleyebilmek için, geride bıraktıkları izleri silmeye çalıştıkları görülmüştür (Bıçakcı, 2012: 214).

Siber güvenlik; İnsan faktörü, teknoloji ve eğitim unsurları çerçevesinde yönetilmesi gereken ve nispeten karmaşık aşamalardan oluşan süreklilik arz eden bir süreçtir. Bu üç unsur arasında bütünlük olmadıkça yüksek seviyede bir güvenlikten bahsedebilmek mümkün değildir.

Güvenliğin en zayıf halkası olan personelin eğitimi sağlanmalı ve kendi içinde çalışan bir otokontrol sistemi kurulmalıdır. Bireysel ve kurumsal anlamda, konu ile ilgili yüksek farkındalığın olması ve gerekli tedbirleri alabilecek uzman yöneticilerin kurumlarda bulunması gereklidir. Ağa bağlı tüm sistemlerin güvenliğinin alınmasının sağlanması ve neyin ne dereceye kadar korunması gerektiğinin bilinmesi, bilgi güvenliğindeki en önemli adımı oluşturmaktadır. Her aşamada izleme ve denetim sistemleri kurulmalı ve sağlıklı bir geri bildirimle tekrar gerekli tedbirler gözden geçirilmelidir. Siber saldırılara karşı mücadele çalışmaları göstermiştir ki, en büyük ve gerçek tehdit bilinmezlikten, bilgi eksikliğinden ve yanlış bilgilerden kaynaklanmaktadır (Alnıak, 2004: 2). Siber güvenlik günümüzde ihtiyaçtan ziyade bir zorunluluk olmuştur. Siber güvenliğin, dağınık, birbirinden habersiz ve eşgüdümsüz, gerçeklerden ve güncel uygulama örneklerinden uzak bir şekilde sağlanabilmesi mümkün değildir (Alkan vd., 2012: 5).

Yüksek seviyede saldırılara hazırlıklı olabilmek için kurumsal, bireysel ve yönetimsel anlamda, siber güvenliğin sağlanabilmesi adına, gerekli tedbirlerin alınması

sağlanmalıdır. Şimdi, siber güvenliğin kademeli olarak sağlanabilmesi için, sırasıyla Bireysel, Kurumsal ve Devlet Yönetimi başlıklarında alınması gereken tedbirler incelenecektir (Sağıroğlu, 2013: 95).

6.3.1. Bireysel Anlamda Alınması Gereken Tedbirler

Siber ülke güvenliğinin sağlanması, bilişim teknolojilerini kullanan en küçük yapı taşı olan insan ve onun çevresinden başlar. Sistemlere nüfus eden küçük sistemlerin ve onu kullanan kullanıcıların basit önlemleri almaması sebebiyle sunulan hizmette kesintiler ve hatta duraksamalar yaşanabilmektedir.

Tablo 6: Bireylerin Bilişim Güvenliği Ürünleri Kullanım Oranı ve Türleri (%)

	Türkiye	Kent	Kır
Güvenlik ürünleri kullanımı	57,4	61,0	39,1
Güvenlik ürünü kullananların kullandıkları güvenlik türleri			
Bir virüs koruma ve / veya casus yazılım engelleyici (anti spyware) yazılımı	79,3	79,7	76,2
Donanım ya da yazılım olarak güvenlik duvarı (firewall)	38,7	39,6	31,7
İstenmeyen e- postaları (spam) engellemek için e-posta filtresi	16,0	16,2	14,1
Ebeveyn kontrolü ya da web filtreleme yazılımı	5,5	5,5	5,6
Bir paket olarak var ama içeriği bilinmiyor	15,7	15,2	20,1

Kaynak: DPT, 2011.

Tablo 6 incelendiğinde Türkiye'de Nisan 2011 – Mart 2012 tarihleri arasında bilişim güvenliği ürünleri kullanım oranlarına baktığımızda, bireylerin sadece %57,4'ünde herhangi bir güvenlik ürününün kullanıldığını görüyoruz. Sırasıyla alınan güvenlik önlemi yöntemlerine bakıldığında, anti-virüs veya casus engelleyici yazılımın %79,3 ile en çok talep edilen ve kullanılan güvenlik ürünü olduğunu sonrasında ise %38,7 ile güvenlik duvarı kullanımının geldiğini görüyoruz. Siber güvenliğin

sağlanması adına en önemli adım, bireysel önlemler aşamasında gelmektedir. Bu aşamada bireysel anlamda alınabilecek temel güvenlik tedbirlerini sıralayacak olursak;

6.3.1.1 Anti-Virüs Programları

Başlangıçta kendi kendini kopyalayan zararsız ufak programcıklar olarak ortaya çıkmış olsalar da, günümüzde etki ettiği sistemin donanımına zarar verebilecek yetenekleri olan virüsler bulunmaktadır. Bireysel anlamda, siber güvenlik tedbiri olarak alınabilecek en temel ve başlıca önlem, işletim sistemi barındıran tüm elektronik cihazlara, güvenilirliğini kanıtlamış bir anti-virüs programı yüklemektir. Günümüzde NATO gibi uluslararası büyük kuruluşlar, kendi personeline dahi evindeki cihazlarında kullanabileceği anti-virüs yazılımlarını ücretsiz olarak sağlamaktadırlar. Çünkü kurum ve kuruluşların güvenliği de bu kurumda çalışan personellerden başlamaktadır. Bu günün güncel anti-virüs programının yarının virüslerine karşı güncel olamayacağı unutulmamalıdır. Bu nedenle mevcut anti-virüs programlarını sürekli güncel tutmak, yazılımı yayımlayan firma tarafından yayımlanmış güncelleme ve yama paketlerini yüklemek gerekmektedir. Artık günümüzdeki çoğu anti-virüs yazılımı mevcut olan çeşitli saldırıları önleyebilmekte ve kullanıcılara tam olmasa da nispeten iyi bir güvenlik ortamı sağlayabilmektedir.

6.3.1.2 Güvenlik Duvarı

Önceleri Şirket, Kurum ve Kuruluşların büyük bilgi sistem ağ yapılarında kullanılan güvenlik duvarları, artık bireysel güvenliğin sağlanması amacıyla da tercih edilmektedir. Güvenlik duvarları; geniş alan ağına erişimlerin güvenliğini ve kontrolünü sağlamada, geniş alan ağında hizmet sunan servislerin yetkilendirilmesinde ve bu sistemlere içeriden erişimlerin kontrolünün ve güvenliğinin sağlanması için kullanılan, donanım veya yazılım tabanlı cihaz/programlara verilen genel adıdır. Ateş duvarı veya ingilizce ismiyle firewall olarak adlandırılır. Günümüzde donanımsal ve yazılımsal versiyonları bulunan güvenlik duvarları, bağlı olduğumuz ağa kimlerin erişebileceğine, iç ağdan bağlı olan dış ağa kimlerin çıkabileceğine, hangi yazılımların çalışmasına izin

verilebileceğine kadar detaylandırılabilecek birçok güvenlik önleminin alınmasını sağladıklarından dolayı, birinci aşama güvenlik tedbiri olarak kullanılacak en temel bileşen olarak kabul edilmektedir. Ağ erişimine ve kullanımına yetkilendirmenin ilk aşaması olarak kabul edilen güvenlik duvarları, bireysel anlamda siber güvenliği sağlamada çok önemli bir yere sahiptirler (http://en.wikipedia.org, 23.03.2013).

6.3.1.3 Güvenlik Yamaları

Kullanılan işletim sisteminde tespit edilen güvenlik açıklarını kapatan, sistemin daha kararlı ve doğru çalışmasını sağlayacak olan güncelleme veya yama paketleri, yetkili firmalar tarafından hazırlanarak internet üzerinden veya cd ortamından kullanıcılara yayımlanmaktadır. Önemli güvenlik açıklarının giderilmesini sağlayan bu güncelleme paketleri, kişisel ve kurumsal güvenliğimiz açısından önemlidir. İfşa edilen bir sistem açığı, bu açığı kullanan korsan saldırganlar tarafından, başka kapıların açılmasına ve böylelikle sistemin ele geçirilmesine sebep olabilmektedir. Günümüz teknolojileri sayesinde, yayımlanan yama ve güncellemeleri otomatik olarak yüklemek mümkündür. Yeni alınan veya yeni yüklenen bir işletim sisteminden sonra ilk yapılması gereken, yayımlanmış olan güncellemelerin sisteme yüklenmesini sağlamaktır.

6.3.1.4 Parola Güvenliği

Parola veya şifrelerle güvenliğin sağlanmaya çalışılmasının kolay ve ucuz olması nedeniyle, parolalar halen günümüzde en çok tercih edilen güvenlik araçlarıdır. Çoğu internet sayfalarında kullanıcı doğrulama işlemleri şifrelerle yapılmaktadır. Sürekli aynı parolanın kullanılması, sistemi izleyen veya kontrol eden kişilerin parolaları elde etmesine imkan sağlamaktadır. Bu güvenlik açığının üzerinden gelebilmek için, özellikle bankacılık hizmetleri gibi internet üzerinden hizmet veren şirketler, her seferinde farklı şifre üreten OTP(Tek kullanımlık şifre) cihazları kullanmaktadırlar. Geleneksel şifreleme tekniği kullanan sistemlerin parola güvenliğini sağlayabilmeleri için parolanın uzun olması, tekrar eden rakamlardan oluşmaması, kolay tahmin edilen doğum tarihi veya yılı gibi rakamlardan oluşmaması, sürekli aynı parolanın kullanılması

yerine belirli aralıklarla değişen parolaların kullanılması gerekmektedir. Her sistemde olduğu gibi parola güvenliğinde de en zayıf halka insandır. Unutmamak amacıyla bir yere yazılan parolalar çok kolay elde edilebilmektedir. Saldırganların geliştirdiği deneme programcıkları sayesinde, parolaları ele geçirmeye yönelik saldırılar günümüzde sıkça olmaktadır. Sözlük saldırıları şeklinde olan bu saldırılarda, saldırgan sözlükteki tüm kelimeleri bir program sayesinde deneyerek parolayı bulmaya çalışmaktadır. Bu tarz saldırılardan korunmak için karmaşık harflerden, büyük veya küçük harflerden oluşan, içerisinde rakam ve karakter içeren parolalar belirlenmelidir. Sisteme, en fazla yanlış girilebilecek parola deneme sayısı da belirtilerek korunma sağlanmalıdır (Hub, 2011: 437-440).

6.3.1.5 Elektronik Posta Güvenliği

Bilişim toplumunun insanoğluna sunduğu güzel hizmetlerden birisi de hiç şüphesiz elektronik posta hizmetidir. İstediğiniz her internet noktasından posta kutunuza bağlanarak, adınıza gönderilmiş elektronik mektupları kontrol etme şansımız sayesinde, mobil ve hareketli dünyamızda, e-posta uygulamaları bizi, mektupla haberleşmede bir noktaya bağımlılıktan kurtarmaktadır. Milyonlarca dolarlık zararlara sebep olan virüs saldırılarının e-postaları kullanarak yayılması, e-posta kullanımının popülerliğinin bir göstergesidir. E-posta kullanımı bireysellikten de çıkarak artık kurumsal hale gelmiştir. Çoğu kamu kurum ve kuruluşları ile e-posta adresleri üzerinden resmi olarak haberleşmemiz sayesinde, E-Devlet modelinin insanlara sağladığı hızlı ve kolay iletişimi de gerçekleştirmiş oluyoruz. Dolayısıyla göndermiş veya almış olduğumuz e-postaların güvenliği, kişisel ve kurumsal güvenliği önemli ölçüde ilgilendirmektedir. Gönderilen bir e-posta, çıkış noktasından ilgili kişiye ulaşıncaya kadar çok rahatlıkla okunabilir. Bazı korsan yazılımlar sayesinde gönderenin kimliği değişikliğe uğratılabilinir. S/MIME ve PGP gibi e-posta güvenliği üzerinde çalışan sertifika ve yazılımlar olsa dahi, e-posta güvenliğinin tam olarak sağlanabileceği iddia edilmesi zordur. Buna rağmen kurumsal ve bireysel anlamda alınabilecek temel tedbirler bulunmaktadır. Bunların başında e-posta hizmeti sunan servislerin, kamu kurum ve kuruluşları açısından kendilerince işletilen servisler olmasına, bireysel e-posta hesaplarında ise kendisini ispatlamış yerli firmalarca işletilen e-posta hesaplarının

kullanılmasına dikkat edilmelidir. Bilinmeyen kişi veya gruplardan gelen e-postalara daima şüpheyle yaklaşılmalı, hatta okunmadan silinmeli, bireysel ve kurumsal e-posta hesapları birbirinden ayrılmalıdır. İnternet sayfalarına veya gruplarına üye olunurken kullanılan parolalar ile e-posta parolaları birbirinden farklı olmasına dikkat edilmelidir. İstihbarat birimlerince e-posta hesaplarının kontrol edildiğine, içinde bazı kelimeler geçen e-postaların özel olarak okunup takip edildiğine dair iddialar bulunsa da henüz kanıtlanamamıştır (Levi, 2012).

6.3.1.6 Kablosuz Ağ Güvenliği

Kablolu bağlantıya oranla kurulumunun kolay olması, fiyatının ucuz olması, rahatlıkla yeniden konumlandırılabilmesi, hat veya kablo çekme gibi masraf ve zahmetlerinin olmamasından dolayı kablosuz iletişim aygıtları her geçen gün daha fazla talep edilmektedir. Sistemi oluşturan kablosuz ağ modemi veya kablosuz yönlendirici sayesinde, hızlı bir paylaşım ortamı oluşturulabilmektedir. Buna rağmen kablosuz ağ bağlantıları, bilişim sektöründe, yapılan yayınının kapsama anındaki herkes tarafından görebilmesi sebebiyle, en güvensiz ağ ortamı olarak görülmektedir. Kablosuz yayın içerisindeki haberleşmeleri okuyan yazılımlar ve sistemler sayesinde korsan saldırganlar kolaylıkla ağ ortamındaki verilere erişebilmektedir. Siber saldırı yapabilmek için kapsama alanı içerisinde bulunmak yeterlidir. Kimi zaman bu kapsama alanına yapılacak erişim bir otopark, bitişikteki ev, kafeterya, bekleme salonu olabileceği gibi, gelişmiş anten sistemleri kullanılarak, nispeten uzaktaki kablosuz ağlara da saldırılar düzenlenebilmektedir. Yapılan bir çalışmada, uzaktan yönetilmiş bir bilgisayar sayesinde, 30 km uzaktan bir kablosuz ağa saldırı düzenlenebilmiştir. Güvenliği arttırıcı ek özellikler zamanla kablosuz ağ cihazlarına ilave edilmiş olsa da, kritik bilgi işlenen ağ ortamlarında, kablosuz iletişim ortamının kullanılmasında sakınca vardır. Cihazların üzerindeki çeşitli güvenlik önlemleri, varsayılan olarak fabrika çıkışında pasif hale getirildiğinden, kullanımdan önce yetkili personel tarafından aktif hale getirilmesi gerekmektedir. Kablosuz ağ ortamlarında, güvenliğini sağlamak amacıyla alınması gereken başlıca önlemleri şu şekilde sıralayabiliriz;

- Kablosuz yayın yapan modem veya yönlendirici cihazın ayarlarından, yapılan kablosuz ağ ismi (SSID) yayının herkese görünecek şekilde yapılmaması sağlanmalı,
- Kablosuz ağ erişimi için algoritması kuvvetli anahtarlama sistemleri tercih edilerek, kablosuz ağa şifre verilmeli,
- Gelişmiş ağ filtreleme tabloları (MAC Filtreleme) kullanılarak, erişim kontrolünün yapılması sağlanmalı,
- Kablosuz ağ bağlantı noktaları bina veya erişim alanının ortasında bir yere konumlandırılmalı, böylelikle bina dışına veya kullanım alanı dışına kablosuz ağ yayının gitmesi önlenmelidir,
- Kablosuz ağ ortamında kritik ve gizli bilgilerin işlenmemesine dikkat edilmeli,
- Kablosuz ağ ortamını oluşturan tüm cihazların fabrika ayarlarıyla gelen standart şifrelerinin, sistemi kurar kurmaz değiştirilmesi ve güvenli bir şekilde muhafaza edilmesi sağlanmalı,
- Kablosuz ağ cihazlarına fiziksel erişimi engelleyebilecek fiziksel güvenlik önlemlerinin alınması,
- Kullanıcılara, ağ ortamının güvenli olmadığı hatırlatılarak, önemli verinin işlenmemesi gerektiği aktarılmalıdır (Loo, 2008: 66-71).

6.3.2. Kurumsal Anlamda Alınması Gereken Tedbirleri

Siber tehdidin her geçen gün sürekli değişmesi ve bir önceki halinden daha karmaşık, daha güçlü bir hal alması sebebiyle, alınacak tedbirlerin dinamik olması gerekmektedir. Bu yönüyle siber tehdit, diğer tehditlerden farklı olarak, sürekli takip ve izlemeyi gerektirmektedir. Sistemlerin güncel tehditlere karşı güvenilir hale gelebilmesinin sağlanması ve karşı reaksiyon gösterilebilmesi adına, sürekli takip gerektiren bir yapının kurulması gereklidir Siber saldırılar sadece askeri hedeflere yönelik olmamaktadır. Saldırıların organize oluşu ve nereden geldiğinin bilinememesi sebebiyle, öncelikle ülke içerisindeki kamu kurum ve kuruluşları ve özel sektör

firmalarıyla başlayan sonrasında dünya çapında, diğer ülke ve kurumlarla işbirliği ve koordinasyonun sağlanması önem arz etmektedir (Bıçakcı, 2012: 223).

Bilgi güvenliğinin sağlanması için, teknik çözümlere yüksek miktarda yatırım yapan kurumlar ve şirketler, genel anlamda insan faktörüne gerekli önemi vermemektedir. Teknik önlemlerin teknolojik imkanlar doğrultusunda sağlanması, bilgi güvenliğinin tesis edilmesi açısından önemli olmasına rağmen, kullanıcı bilincinin de kazandırılması gerekmektedir. Kullanıcıları, almaları gereken güvenlik önlemleri hakkında hazırlamanın en önemli yolu, eğitimleri bir plan doğrultusunda yapmaktan geçmektedir. Konusuna hakim, yeterli teknik bilgiye sahip kişiler tarafından, sistematik bir planda yapılan bilinçli eğitimler, bir çok güvenlik ihlalinin daha olamadan önüne geçebilmektedir. Kurum ve kuruluşların yönetici kadrolarına, bu eğitimlerin takip ve kontrolünde önemli görevler düşmektedir. Kuruma yeni başlayan her personele, hangi konularda yetkili olduğu ve dikkat etmesi gereken hususların belirtildiği katılış sunumu gibi başlangıç eğitimlerinden sonra periyodik eğitimlerin (Aylık, 3 Aylık, 6 Aylık) verilmesi bilgi güvenliği farkındalığı için önemlidir. Bu eğitimlerin devamında, eğitim sonuçları değerlendirerek, eğitimi revize etmek veya tekrarlamak, eğitim içeriğini geriye dönük olacak şekilde güncellemek, eğitimin kalitesi açısından önemlidir. Genel bir bilgi güvenliği farkındalığı tesis edebilmek için başlıca aşağıda sunulan konuların eğitimlerde en temel seviyeden ileri düzeye kadar öğretilmesi faydalı olacaktır.

- Şirket / Kamu Kurum veya Kuruluşlarının güvenlik politikalarının ne olduğunun ve nasıl uygulandığının belirtilmesi,
- Kullanıcı Adı ve Şifre gibi temel kişisel güvenlik bilgilerinin nasıl teşkil edilmesi ve ne şekilde muhafaza edilmesi gerektiği gibi bilgilendirmeler,
- E-posta ve interneti, zararlı yazılımların etkisine maruz kalmadan amacına yönelik olarak kullanımı konularında bilgilendirme,
- Giderek artan oranda günlük hayatımızda kullanılan, mobil cihazların oluşturduğu güvenlik riskleri ve bunların önlenmesi,
- Virüsler, hırsızlık veya olağan dışı bilgisayar hareketliliğinin yetkili kişilere nasıl bildirileceği, ne gibi önlemler alınacağı.

Yukarıda bahsedilen hususların eğitimlerde kullanıcılara verilmesi, kurumsal bilgi güvenliği bilincinin oluşturulması açısından önemli olmakla birlikte eğitimlerin

içerikleri kurum ve kuruluşların çalışma alanları doğrultusunda detaylandırılabilinir. Bu eğitimleri temel amacı, kurum içerisindeki veri bütünlüğünü ve gizliliğini sağlamak, elektronik haberleşme sistemlerini verimli ve etkili kullanmak, kurum içi donanım ve yazılım güvenliğini sağlamak, bireysel farkındalık bilincini aşılamak, kaynakların etkin ve verimli bir şekilde kullanılmasını sağlamaktır (Gökçe, 2010).

Yedekleme Sistemleri; Kamu kurum ve kuruluşlarında hizmet veren her türlü E-Devlet uygulamasının, verilerinin belirli aralıklarla yedeklenmesi, bilginin güvenliği ve korunması açısından son derece önemlidir. Siber saldırılar ve savaşlar sonucu kaybolan veya bozulan verinin yerine, en son yedeklenmiş verinin hizmete sokulması sayesinde, E-Devlet uygulaması veya hizmeti, saldırı sonrası hizmet vermeye kısa sürede başlayacaktır. Kurumsal anlamda yedekleme işlemlerinin merkezi olarak yapılması ve muhafaza edilmesi, verinin bütünlüğünü ve güvenliğini korumak adına önemlidir. Merkezi teşkilatın, bu görevi yerine getirmesi halinde taşra teşkilatlarındaki olası veri kayıpları önlenebilir. Yedekleme hizmetlerinin yerine getirilmesi için, yazılımsal ve donanımsal bir çok ürün bulunmaktadır. Saklanacak verinin büyüklüğüne, alınacak yedeğin sayısına ve periyoduna bağlı olarak çeşitli sistemlerden yararlanmak mümkündür. E-Devlet uygulamaları veya bunun yanında devam eden hizmetlerinden dolayı oluşan verilerin arşivlenmesi işlemi daima kontrollü ve birden fazla kademece yapılmalıdır. Olası veri kayıplarının önüne geçmek için, kurum ve kuruşların bilgi sistem yöneticileri de kendi yedeklerini tutabilmelidir.

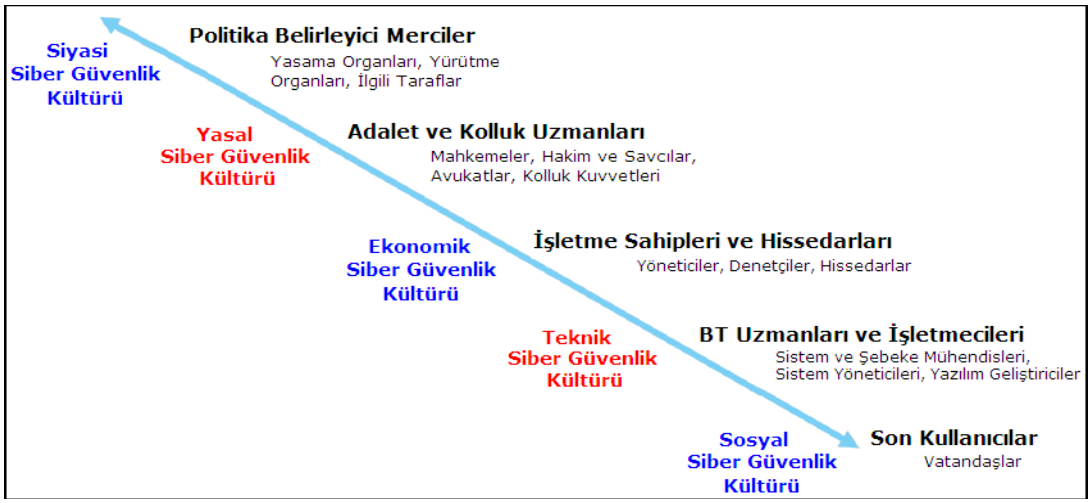
6.3.3. Devlet Yönetimi Anlamında Alınması Gereken Tedbirler

Öncelikle tüm siber güvenlik tedbirlerini içeren, siber güvenlikte ülke olarak hedefini belirten bir ulusal siber güvenlik politikası ve siber güvenlik stratejisi geliştirilmelidir. Kurumlar arası siber güvenliği sağlayacak ve koordine edecek bir birimin gerekli yetkilerle birlikte kurulması, siber güvenlikle mücadele amacıyla yasal çerçevenin oluşturulması gerekmektedir. Siber suçlarla mücadele biriminin kurulması veya mevcut yapıların resmileştirilmesi bu alandaki mücadeleye olumlu katkı sağlayacaktır. Toplumsal farkındalığın artırılabilmesi için bilgi güvenliği eğitimi tüm kademedeki bireylere verilmelidir. Uluslararası işbirliğinin arttırılmasına yönelik

adımların atılması gerekmektedir. Uluslararası kabul görmüş Bilgi Güvenlik Sistemleri Standartları'nın E-Devlet hizmeti sunan devlet kurumlarında zorunlu hale getirilmesi sağlanmalıdır. Bu konuda yapılan/yapılacak olan arge çalışmaları desteklenmelidir. Edinilen tecrübeler doğrultusunda farkına varılan açıkları, en kısa sürede giderebilecek yapısal bir sistemin sürekli çalışabilecek şekilde kurulması gereklidir (Sağıroğlu, 2013: 89-98).

E-Devlet hizmetlerinin klasik devlet hizmetlerine nazaran fiziksel açıdan daha soyut olması sebebiyle, e-ortamda hata yapma riski daha yüksek ve yapılan işlemin kontrol edilmesi olanağı daha düşüktür. Tüm işlemlerin bilgi sistem ortamları üzerinden gerçekleşmesi bakımından E-Devletle beraber neyin nasıl yapılması gerektiğine dair sağlam temellere oturtulmuş politikalar ve stratejiler geliştirilmelidir. E-Devlet bilgi ve belgelerinin güvenliğinin sağlanması açısından, veri kurtarma ve yetkilendirme temelli bir sistem üzerinde çalışan, kontrollü, gerekli risk analizlerinden geçmiş güvenli ve merkezi bir belge yönetim sistemi gereklidir. Bu belge yönetim sistemi, zaman ve personel tasarrufunun yanında çeşitli istek ve beklentilere kolaylıkla uyum sağlayabilecek şekilde esnek olmalı, diğer ulusal sistemlerle kolaylıkla veri alışverişinde bulunabilecek bir yapıda teşkil edilmelidir (Altın, 2008: 284-285).

Tablo 7: Siber Güvenlik Kültürünün Oluşturulması



Kaynak : ITU, 2011.

Devlet yönetiminin siber ülke güvenliğini sağlayabilmesi için öncelikle toplumda siber güvenlik kültürünü geliştirmesi gereklidir. Tablo 7'de siber güvenlik kültürünün vatandaşlardan başlayarak politika belirleyici mercilere kadar uzanan aşamaları gösterilmiştir. Siber güvenlik kültürü sosyal, teknik, ekonomik, yasal ve siyasi katmanlardan oluşmaktadır. Her katmanın üzerine düşen belli başlı görevleri bulunmaktadır. Siber güvenlik kültürünün oluşturulması, bu katmanların birbiriyle eşgüdümlü bir şekilde çalışması ve koordinesiyle mümkün olur. Yukarıda değinilen önlemlerin yanında, bir ülkenin veya ulusun kritik öncelikte olan altyapılarıyla birlikte hizmet olarak sunduğu E-Devlet uygulamalarının korunması ve güvenliğinin sağlanabilmesi için dört temel konuda hazırlıklı olması gerekmektedir (Itu, 2011). Bunlar;

a) Siber Savunma Yoluyla Korunma,
b) Siber Caydırıcılık,
c) Siber Saldırının Duraklatılması veya Hasarın Sınırlandırılması,
d) Siber Savaş Görev Kuvveti'dir.

6.3.3.1. Siber Savunma Yoluyla Korunma

En temel ve basit seviyede bir bireysel siber savunma, sistem üzerine kurulan anti-virüs yazılımıyla sağlanabilirken, gelişmiş alt yapıya sahip karmaşık sistemlerin savunma mekanizmaları da karmaşık olmaktadır. Günümüzde en son güvenlik sistemiyle donatılmış olsa dahi, bugünün korunaklı sistemleri yarının gelişmiş siber saldırılarından etkilenmeyecek anlamına gelmemektedir. İnternet üzerinden sağlanan servislerde yapısal olarak, hassas bilginin üzerinde bulunmamasına dikkat edilmeli, sistemler üzerinde gereksiz detay veri veya bilgiler bulunmamalıdır. Çalışan her bir sistem ve çıktısı, istenmeyen ellerin eline geçmesi durumunda nasıl bir etki/tesiri olabileceği değerlendirilerek incelenmeli, amaca yönelik olmayan detay veriler erişime engellenmelidir. Gelişmiş şifreleme ve kimlik tespit etme yazılımları ile gelen ve giden tüm ağ paketleri kontrol edilmeli ve yetkili olan personellerin kimlik kontrolleri sonucu erişimlerine izin verilmelidir. Günümüzde mevcut olan arşivleme ve erişim kontrolü yazılımları ile tüm sisteme erişimin, kimler tarafından, ne zaman, nereden ve hangi ip adresi üzerinden erişildiğinin bilgileri tutulabilmekte ve ileride olabilecek herhangi bir

ihlalde/saldırıda bu verilerden faydalanılmalıdır. Kurumca elde edilmiş güvenlik seviyesine her zaman şüphe ile bakılmalı, hiçbir zaman mevcut tedbirlerin yeterli olduğu düşünülmemelidir. Teknolojik gelişmeler yakinen takip edilmeli, sistemin yapısı da bu gelişmeler paralelinde güncellenmelidir. Siber savunma argümanları tek başına olası saldırıları engellemeye yeterli değildir. Savunma tertiplenmesi belirgin düşmanlardan ziyade, belirgin tekniklere dayalı geliştirildiğinden dolayı düşman veya korsanlar her zaman saldıracak başka bir açık bulabilmektedir. Elektronik sistemleri sadece siber savunma mekanizmalarıyla donatılmış olarak tutmak, tehditleri azaltsa da bitirmeyecektir. Hizmet veren sistemlere bir şekilde dışardan erişmek gerekmektedir. Günümüzde dışarıdan erişimlerde yetkili veya yasal bir kullanıcı gibi kendisini gizleyebilen siber korsanlar her zaman vardır ve olacaktır (Lin, 2012: 75-87).

6.3.3.2. Siber Caydırıcılık

Soğuk savaş dönemlerinden günümüze bir devletin savaş caydırıcılığı elinde bulundurduğu nükleer silah kabiliyeti ile doğrudan ilişkili olarak süregelmiştir. Savaş caydırıcılığı yüksek olan nükleer silahların yerine siber uzayda, saldırı kabiliyeti geniş ölçüde caydırıcılık olarak değerlendirilmektedir. Nükleer silahın tersine, siber saldırıların nereden ve hangi ülkeden nasıl geleceği halen bilinememektedir. Bu da ülkeler açısından siber saldırının caydırıcı bir etken olarak kullanabileceği anlamı taşımaktadır. Siber savunma ve karşı saldırı kabiliyeti yüksek hemen hemen her ülke, saldıran casus/korsan yapılar için daima risk içermektedir. Siber hazırlık seviyesi ne kadar yüksek olursa bu caydırıcılık da o derece artmaktadır. Mevcut politikaların, olası siber saldırıların tespitinde ne gibi bir karşılık verileceğine dair yasal mevzuat da bu caydırıcılığa katkı sağlamaktadır. ABD'de olduğu gibi olası siber saldırıların yerlerinin tespit edilmesi durumunda, bu saldırılara güç kullanarak istenen yer ve zamanda karşılık verileceğine dair ABD Beyaz Saray Başkanlığı tarafından 2011 yılında yayımlanmış olan siber uzay strateji bildirisi, siber caydırıcılık konusunda örnek olarak gösterilebilinir. Meşru müdafaa hakkını kullanabileceği düşünülen ülkelerde, siber saldırı veya savaş olma olasılığı daha azdır (Lin, 2012: 75-87).

6.3.3.3. Siber Saldırının Sezilmesi, Duraklatılması veya Hasarın Sınırlandırılması

Siber saldırıya maruz kalabilme riski ülkeler için her zaman vardır, lakin bazı politik veya diplomatik husumetlerde taraflar birbirlerine karşı önleyici siber güvenlik tedbirleri alabilir. Bu tarz, olası düşman konumlarına karşı alınmış olan erken önlem, muhtemel saldırıyı engelleyebileceği gibi psikolojik üstünlüğün de elde edilmesini sağlayabilir. Siber saldırıya maruz kalındığı andan itibaren yapılması gereken bu saldırının durdurulması veya olası etkilerinin en aza indirilmesidir. Alınacak temel bilgi sistem korunma tedbirleriyle, saldırı metotlarına göre, karşı hamleler atılmalıdır. Ülke yönetim karar mekanizmalarının bu tarz adımları atabilecek önceden yetkilendirilmiş birimlere sahip olması gereklidir. Siber güvenliğin ülke çapında sağlanması için kriz öncesi yürürlükte olan güvenlik politikalarının bu kararları almaya yetkili birimleri de kapsayacak şekilde güncel ve yürürlükte olması, olası siber terör veya saldırı durumunda organize bir savunma politikası açısından önemlidir. Saldırı hazırlığı içerisinde olduğu istihbarat çalışmalarıyla hissedilmiş bir ülkeye karşı yapılabilecek karşı saldırı olası siber savaşın şiddetini azaltacaktır. Düşman ülke veya gurupların, saldırı hazırlıklarını tersine çevirerek ve onları savunmaya yönlendirecek olan karşı saldırı, ülke sistemlerini korumak adına avantaj sağlayacaktır (Lin, 2012: 75-87).

6.3.3.4. Siber Savaş Görev Kuvveti

Ülkeler adına, ülke menfaatlerini korumak ve kollamak için görev yapan, siber uzay ve derinliklerinde her türlü saldırı ve savunma görevinde çalışabilecek, konusuna hakim Siber Savaş Kuvveti'nin hazır bulundurulması önemlidir. Bu görev kuvveti üzerinden yapılacak saldırı senaryosunda, güvenlik kontrol testleri, ülkelerin mevcut durumlarını görebilmeleri açısından gereklidir. Rusya gibi ülkelerde devlet teşviki ile gerçekleştirilen siber korsan saldırı yarışmaları, bu konuya yatkın ve yetenekli kişilerin tespit edilmesine olanak sağlamakta ve bu yeteneklerin yasal sisteme kazandırılması gerçekleştirilmektedir. Günümüzde artık siber caydırıcılığın sağlanması adına bu şekilde görev yapan birimler, ülkeler tarafından gizlenmemektedir. Ülkemizde de siber

güvenliğin sağlanması adına 2012 yılında TSK Siber Savunma Merkezi Başkanlığı teşkil edilmiştir (www.tsk.tr, 22.01.2013).

E-Devlet yoluyla vatandaşa sağlanan hizmetin kesintiye uğramaması için alınması gereken çoğu tedbir, yüksek maliyet gerektirmektedir. Devletler açısından, korunmasız olduğu düşünülen yerden başlanarak, tüm kamu kurum ve kuruluşlarını aynı güvenlik şemsiyesi altında, dış saldırılardan koruyacak siber güvenlik tedbir ve politikalarının en üst mercilerce ele alınıp titizlikle uygulanması gerekmektedir.

GENEL DEĞERLENDİRME

Bu bölüm, araştırma sırasında elde edilen bulgular, bu bulgulara getirilen öneriler ve sonuç bölümünden oluşmuştur.

7. BULGULAR, ÖNERİLER VE GENEL SONUÇ

Çalışmanın bu bölümünde, araştırma sırasında elde edilen bulgular, bu bulgulara getirilen öneriler açıklanmış ve genel olarak bir değerlendirme yapılmıştır.

7.1. Bulgular ve Öneriler

Bulgu (1): Tarım toplumundan sanayi toplumuna, sanayi toplumundan da bilgi toplumuna dönüşüm süreci devam ederken devletlerin de bu doğrultuda değişmesi ve dönüşmesi kaçınılmazdır.

Öneri (1): Toplumsal yaşamın bir zorunluluğu olarak ortaya çıkan devlet kavramı, temel anlamda, vatandaşlarının istek ve gereksinimlerine tatmin edici çözümler bulmak ve hizmet vermekle yükümlüdür. Küreselleşen dünya, hızlı bir değişim sürecinin içinde olduğundan, özellikle bilişim teknolojilerinin hızlı gelişimi, devletlerin toplumlarına ve kurumlarına vermek zorunda oldukları hizmetlerin de değiştirilmesi gerekliliğini ortaya çıkarmıştır. Toplumları oluşturan bireyleri etkileyen büyük değişim ve dönüşümler, bireyleri demokratik yollarla yöneten hükümetleri de etkilemektedir. Bireysel istek ve arzular gelişen teknolojik imkan ve kabiliyetlerin de katkısıyla değişmiştir. Bireyler, teknolojinin insan hayatına kattığı kolaylıkların bir benzerini devlet yönetiminde de görme arzusu içerisindedirler. Dolayısı ile ülke yönetimleri de bu istek ve talepler doğrultusunda değişmek ve zamana ayak uydurmak zorundadır.

Bulgu (2): Bilgi toplumunda, bilgi anlamlı tek kaynak olarak benimsenmekte, geleneksel üretim faktörleri yani doğal kaynaklar, emek ve sermaye ikinci plana düşmektedir.

Öneri (2): Tarım toplumu, sanayi toplumu ve bilgi toplumu eksenine göz attığımızda tarım ve sanayinin bu toplumların temelini oluşturan üretim süreçleri ile

doğrudan bağlantısı göze çarpar. Oysa bilgi toplumunda üretim doğrudan bilgi kullanımı ile değil; bilgi kullanımıyla zenginleştirilmiş ve etkinleştirilmiş bir şekilde, ama yine tarım ya da sanayi üretim şekillerinden birinde olmaktadır. Bu nedenle geleneksel üretim faktörleri yani doğal kaynaklar, emek ve sermaye ortadan kalkmamakta ancak, ikinci plana düşmektedir.

Bulgu (3): Klasik devlet anlayışının getirdiği bürokratik yapıdan dolayı hantallaşan devlet yapısı, toplumun ihtiyaçlarına ve gereksinimlerine cevap veremez hale gelmiştir. Devletler bilgi ve iletişim teknolojilerinin avantajlarından yararlanarak, dijitalleşmekte ve böylelikle hizmet kalitelerini iyileştirmeyi hedeflemektedirler. Artık teknolojinin ve bilişim sistemlerinin sunduğu avantajlar hizmetlerin daha kolay ve hızlı hizmet sunumunu mümkün hale getirmiştir.

Öneri (3): Vatandaşların, özel kurum ve kuruluşların, hatta birbirinden ayrı yapıda teşkil edilmiş devlet yapılarının kendi aralarındaki iletişimlerini internet üzerinden gerçekleştirmesi zaman ve mekan anlamında büyük avantaj sağlarken, ülke ekonomisi de bu durumdan kazanç elde etmektedir. Elektronik işlemlerin sağladığı aktif hizmet sunumu sayesinde, artık saat sınırı ortadan kalkmakta, bürokratik işlemler en aza inerek evrak getir-götür süreçleri bertaraf edilebilmekte, devlet tarafından üretilen mal ve hizmetlerin, her aşamasında zaman, enerji ve mali tasarruf sağlanabilmektedir.

Bulgu (4): E-Devlet kavramı, kamu kurum ve kuruluşlarıyla yapılan her türlü işlemin, servis veya hizmetin uygun bilişim teknolojileri kullanılarak, elektronik ortamda sürdürülmesidir.

Öneri (4): E-Devlet kavramıyla ilgili yapılmış olan tanımların çoğunun ortak noktası devlet işlerinin elektronik ortamda yapılmasıdır. E-Devlet bir uygulama veyahut bir proje değildir. Sürekli takip ve denetim isteyen, sürekli yenilenmesi ve güncellenmesi gereken bir yaşam biçimidir. Sanılanın aksine E-Devlet sanal devlet anlamına gelmemektedir. Gerçek hayattaki devletin, her geçen gün gelişen ve kullanım oranı artan teknolojik olanakları kullanarak, çağın gereklerine uygun hale gelmesi, klasik devlet yapısının teknoloji paralelinde yeniden yapılandırılmasıdır. E-Devlet klasik devlet anlayışının yerine geçecek bir model yönetim şekli değildir. Aksine E-Devlet uygulamaları ve hizmetleri sayesinde, klasik devlet anlayışı içerisinde sunulan

ürün ve hizmetlerin daha kaliteli, zamanında ve hızlı ulaşmasıyla mevcut yönetimi sağlamlaştıran ve güçlendiren bir yapıya sahiptir.

Bulgu (5): Bilgi güvenliği risklerinden korunmanın en iyi yolu, bilgi teknolojilerine ve alt yapısına çok para harcamaktan geçmektedir.

Öneri (5): Bir sistemin güvenliği onu kullanan ve yöneten kişilerin algı, bilgi ve becerileri doğrultusunda şekillenmekte ve gelişmektedir. Sistemin kendisine para harcamaktan çok, hangi çözümü hangi aşamada ne derecede uygulamak gerektiğini bilmek çok önemlidir. Sistemi güncel ve değişen teknolojik gelişmelere cevap verebilecek nitelikte tutmak, bilgi güvenliğini sağlama açısından bir avantaj olarak görünsede sistemi kullanan kullanıcıların eğitim eksikliği bu avantajı yok edebilmektedir. Son teknolojiyle donatılmış bilgi sistemleri yerine, günün ihtiyaçlarına cevap verebilme kapasitesine sahip sistemler ile bu sistemleri yöneten bilişim sektöründeki personellerin eğitimli olması daha fazla bilgi güvenliği sağlayacaktır.

Bulgu (6): E-Devlet uygulamaları ve hizmetlerinin, kurum, kuruluşlar ile bireyler açısından sayısız faydaları olmasına rağmen, kritik altyapıların siber saldırılara maruz kalabileceği endişesi sebebiyle E-Devletleşme sürecine kuşkuyla bakmak greklidir.

Öneri (6): E-Devlet uygulamalarıyla edinilen kazanımlar ve faydalar hem ülke vatandaşları hem de kamu kurum ve kuruluşları açısından oldukça fazladır. Mevcut tehdit ve tehlike her zaman mevcut olmakla beraber bu tehlikeden korunmak adına E-Devletleşme sürecinden vazgeçilemez. Günümüz küresel ortamında bundan vazgeçmek demek uluslararası rekabette her anlamda geriye düşmek anlamına gelecektir. Bunun yerine bireysel, kurumsal veya ülke yönetimi adına alınacak tedbirlerle tehdit ve olası zararları tam olarak kaldırılamasa da etkisi en aza idrililebilecektir.

Bulgu (7): Kritik altyapıları yöneten uygulamaları veya sistemleri internet üzerinden erişilemeyecek şekilde yapılandırmak, o sistemin güvenliğini sağlamakta ve siber saldırı olasılığını ortadan kaldırmaktadır.

Öneri (7): Kendi iç ağ yapısı altında çalışan sistemler nispeten internet üzerinde hizmet veren diğer sistemlere göre biraz daha güvenli bir ortam sağlıyor olsa da, bu erişilemeyecek veya saldırıda bulunamayacak anlamına gelmemelidir. İran'ın nükleer

tesislerine yapılan STUXNET saldırısı göstermiştir ki kapalı devre sistemlere dahi, yeterli argümanlar (virüs, trojan, solucan v.b.) kullanılarak saldırılabilinmektedir. Sistemin internet üzerinde olup olmadığına bakılmaksızın gerekli güvenlik tedbirleri alınmalı ve her daim hazırlıklı olunmalıdır.

Bulgu (8): Gelişen teklojik buluşlarla halen yaşanmakta olan bilgi toplumu dönüşüm sürecinde, artık bilindik konvansiyonel savaşlar geride kalmıştır. Günümüzde ülkeler ağırlıklarını siber uzaya ve onun sağladığı avatajlarla hasmını egale etmenin peşine düşmüşlerdir. Bundan sonra savaşlar siber ortamda olup sonuçlanacaktır.

Öneri (8): Siber saldırılarla gerçekleştirilen siber savaşlar, saldırı yapan ülkeye, maddi manevi ve aynı zamanda psikolojik birtakım ön avantajlar sağlasa da konvansıyonel savaşın yerine geçebileceği söylenemez. Konvansiyonel savaş öncesi iyi yönetilen ve yönlendirilen bir siber savaş ile hasım ülkenin elektrik, su, haberleşme, ulaşım, finans, sağlık gibi kritik alt yapıları devre dışı bırakılabilir ve bu da olası bir konvansiyonel savaşta, daha başlamadan üstünlük sağlayacaktır.

Bulgu (9): Siber saldırıya maruz kalınması durumunda, ülke olarak alınacak önlemlerin yanında uluslararası iş birliği de önem arz etmektedir. Tam ve zamanında yapılan işbirliği sayesinde saldırının kaynağı tespit edilebilmekte ve saldırının olası etkileri en aza indirilebilmektedir.

Öneri (9): Siber saldırılar internete bağlı herhangi bir lokasyondan kolaylıkla yapılıp yönlendirilebileceğinden dolayı, bu saldırıların kaynağı dünya üzerinde herhangi bir yerden olabilmektedir. Saldırganların IP adresleri üzerinden tespit edilmesi zor ve zaman alan bir süreçtir. Çoğu zaman, saldırının gerçekleştirildiği bilgisayarlar gerçek olmayan sanal IP adresleri aldığından, saldırıların tespiti zorlaşmaktadır. Yapılan siber saldırı anında veya devamında, saldırıya uğrayan sistem veya uygulamaya erişim yerleri dikkatle incelenmeli ve saldırının lokasyonu tespit edilmeye çalışılmalıdır. Bu saldırganların yerinin tespit edilmesinde veya saldırının etkilerinin sistemin çalışmasını etkilemeyecek şekilde en aza indirilmesinde uluslararası işbirliği önemlidir.

7.2. Genel Sonuç

Teknolojinin itici güç olarak yönlendirdiği bilişim toplumu dönüşüm sürecinde, dünyamız gittikçe küresel bir köy haline gelmekte ve bu süreç içerisinde bu zamana kadar süregelmiş olan bireysel alışkanlıklarda değişmektedir. Küreselleşmenin de etkisiyle artık insanlar daha şeffaf bir yönetim, daha adil bir yaşam düzeni, daha hızlı bir kamu hizmetinin yanında açık bir dünya ve eşit eğitim olanaklarını talep etmektedirler. Bu istekler devletleri ve onların yöneticilerini ister istemez bir değişime yönlendirmekte ve bireylerin hayatlarına yansıyan teknolojik kolaylıkları yine onun yardımıyla kamu yönetimine yansıtmaya zorlamaktadır. Bu değişim, bilişim toplumunun isteği doğrultusunda, klasik devlet yönetimi yerine daha fazlasını vaat eden E-Devlet modelinin doğmasını beraberinde getirmektedir.

Tarihsel süreç içerisinde teknolojinin herdaim insanoğlunun hayatına yön verdiği ve onu şekillendirdiği bir gerçektir bu nedenle teknolojinin devlet yönetiminde de etkin bir araç olarak kullanılmasını hedefleyen ülke yöneticileri, kamu yönetiminde daha etkin ve yerinde, sürekli ulaşılabilinir, zaman ve mekan ayrımı olmaksızın hizmet sunumunu gerçekleştiren, maddi ve manevi kazanç sağlayan E-Devlet modelini kamu yönetimine uygulamaya çalışmaktadırlar. Günümüzde kamu dairesine gidilmesi ve bireysel olarak takip edilmesi gereken çoğu işlem bu süreç içerisinde dijitalleşerek internet üzerinden hizmet verir hale gelmiştir. Basit yazılım ve uygulamalarla, vatandaşlar için önemli olan birçok devlet işlemi dijital ortama aktarılmış, ve bir eşgüdüm içerisinde, E-Devlet modeli çerçevesinde kullanılmaya başlamıştır. E-Devletleşme süreci ve teknolojinin de yardımıyla dijitalleşen hizmetler kendisine her geçen gün daha fazla kullanım alanı bulmaktadır. Teknolojinin bu gücünün, kamu yönetimi ve hizmet sunumu alanında E-Devlet modeliyle kullanılması, vatandaşlık bilinci ve bağını arttıracağı gibi, ülke kaynaklarının boş yere israfının da önüne geçeceği değerlendirilmektedir böylelikle yeni devlet yapısının etkin, şeffaf, faydalı ve verimli hizmetler sunabilmesi amacıyla, kamu yönetiminde E-Devletleşme sürecinin kaçınılmaz olduğu hipotezi kendisini doğrulamıştır. E-devlet uygulamalarının hizmet sunumunda aktif olarak kullanılabilmesi için gerek vatandaşların gerekse kamu kurum ve kurumlarının bilgilerine sistem üzerinde ihtiyaç duyulmaktadır. Sistemler bu bilgiler üzerinden kimlik doğrulaması yapmakta, yetkilendirme işlemi gerçekleştirmektedir.

Yine bu uygulamalar içerisinde, e-imza sayesinde, ıslak imzalı belgeler ile gerçekleştirilebilen her türlü işlem, elektronik ortamda da yürütülebilmektedir. Edevlet uygulamaları içerisinde kişisel, kamusal bilgi ve belgelerin yanında devlet sırları gibi ülke güvenliği açısından önemli olan birçok bilgi ve belge de dijital hale getirilmiştir. Yakın geçmişte E-Devlet sistemlerine ve uygulamalarına yapılan bazı siber saldırılar sonrası, bu sistemlerin güvenliği ülkeler bazında sorgulanmaya başlanmıştır. E-Devlet hizmetini yürüten kamu kurum ve kuruluşları veya özel sektör firmaları mevcut siber tehditlere karşı bir takım güvenlik önlemi alsalar da her geçen gün değişik bir takım yolları deneyerek daha da güçlü hale gelen siber saldırı olayları, bu güvenlik önlemlerinin çoğu zaman yetersiz kaldığını göstermiştir. Bununla beraber, E-Devlet uygulamalarıyla sunulan hizmetlerin, toplum nazarında kabul görmesi ve kamu yönetimine getirdiği kolaylıklar sebebiyle toplum tarafından daha fazlasının talep edilmesi, siber güvenlik kaygısını bir müddet göz ardı tutmuş olsa da 2000'li yıllarda yaşanan siber saldırlar ve neticeleri dolayısı ile bu kaygı tekrar gündeme gelmiştir. Uzaktan yönlendirilebilinecek bir siber saldırı ile belki bir bombadan daha fazla hasar ve kaos yaratabilmek mümkün hale gelebilmektedir. Yakın geçmişte yaşanan siber saldırıların çoğunda, zarar verilmek istenen olgu, dijital verilerden oluşan bilgi, belgeler veya parasal değerler olmuşsa da, Stuxnet virüsü bizlere bu zararlı kodların, istenmesi halinde maddi hasar da verebileceğini ve ülke adına hayati öneme sahip proje ve yatırımları kesintiye uğratabileceğini göstermiştir. Stuxnet saldırısında, İran'ın nükleer projesinin gelişimi, sadece bir virüs yardımıyla, bir bombadan daha etkin bir şekilde sabote edilmiştir.

E-Devlet uygulamaları, içerdiği bilgiler ve kullanıcı yoğunluğu da göz önüne alındığında, siber teröristler açısından çok cazip ve potansiyel bir hedeftir. Her ne kadar, (Alnıak, 2004: 1)'ın raporuna göre "2004 yılına kadar kayıtlara geçmiş, teröristler tarafından ulusal altyapıların kritik birimlerine, siber terörizm adını hak edecek derecede, bilinçli ve organize biçimde gerçekleştirilen bir siber saldırının mevcut olmadığı" belirtilmiş olmasına rağmen, sonraki yıllarda yaşanan siber saldırılar, bu saldırıların ne derece hızla gelişebileceğinin ve ne derece kamu düzenini etkileyebileceğinin önemli bir kanıtı olmuştur.

Estonya siber savaşından da öğrenildiği üzere, bilişim sistemleri üzerinde, bilgi sahibi olmayan kişilerin bile organize olarak saldırılara eşlik edebileceği ve bu saldırılar

sonucunda, bir ülkenin E-Devlet uygulamalarının kesintiye uğratılabileceği ispatlanmış ve gelişmekte olan E-Devlet olgusunun önündeki en büyük engelin, siber ülke güvenliği kaygısının olduğunu belirten hipotezimiz kendisini doğrulamıştır. Bilgi güvenliği ve devamında gelen siber güvenlik anlayışı, her an canlı ve zinde tutulması gereken bir güvenlik politikası olmalıdır. Bilgi güvenliği, toplumu oluşturan bireyden başlayarak karar vericilere kadar kademe kademe uzanmaktadır. Her birimin kendi üzerine düşen görev ve sorumlulukları bulunmaktadır. Alınması gereken tedbir ve önlemlerin yerinde, zamanında ve yeteri oranda alınması durumunda, siber saldırıların sistemler üzerinde bırakabileceği hasarların da en aza indirilebilmesi mümkün olabilmektedir.

Toplumdaki genel kanı, büyük alt yapılara sahip önemli hedeflere nazaran küçük kuruluşların, büyük olanlara nispeten daha korunaklı ve daha güvenli olduğu şeklindedir. Aslında bu gerçeği yansıtmamaktadır. Uluslararası bir güvenlik firması olan MacAfee'nin Başkan Yardımcısı Dimitri ALPEROVITCH "…siber saldırılardan ve siber savaş kaygısı yaşamayacak olan tek kurum veya kuruluş, elinde değerli hiçbir veri bulundurmayandır" (Glennon, 2012: 88) diyerek aslında siber saldırılardan korunmanın örgütsel anlamda büyüklük, küçüklük ile alakalı olmadığını, asıl değerlendirilmesi gerekenin elde bulunan veya işlenen verinin önem derecesi olduğunu belirtmektedir. Kuruluşun büyüklüğünden ziyade o organizasyonun nasıl korunduğu ve saldırılara karşı nasıl cevap verdiği önem arz etmektedir. Yapısı itibariyle siber saldırılar uzaktan koordine ve kontrol edilebilmekte, sistem açıkları kullanılarak saldırılan sistemlere zarar verilebilmektedir. Bu saldırıların önlenmesi ve engellenmesinde ulusal siber güvenlik bilincinin oluşmasının yanında, uluslararası işbirliğinin de sağlanması gerekmektedir. Ulusal siber güvenlik algısı için kullanıcılardan sistem yöneticilerine kadar eğitimler verilmeli, tüm siber güvenlik tedbirlerini içeren, siber güvenlikte ülke olarak ulaşılması gereken hedefi belirleyen bir siber güvenlik politikası ve siber güvenlik stratejisi geliştirilmelidir. Bireysel, kurumsal ve devlet adına alınması gereken tedbirler sırasıyla alınmalı ve alınan bu tedbirler belirli aralıklarla gözden geçirilerek zamanın yeni ihtiyaçlarına cevap verebilecek şekilde güncellenmelidir. Siber güvenliğin sağlanmasında kullanıcı eğitimi birinci öncelikte gelmektedir. Siber güvenliği saylayabilmek adına alınması gereken pasif tedbirlerin yanında siber caydırıcılığı pekiştiren aktif adımlar atılmalı ve siber uzayda kazanılan yetekler uluslararası toplumun bilgisine sunulmalıdır. Siber uzayda edinilen başarılar veya kurulan resmi

örgütsel yapılanmalar, saldırganlara göz ardı edilmeyecek bir korku verecektir. Siber saldırıların, siber savunma adına herhangi bir adım atmamış olan ülkelerde daha fazla oranda gerçekleştiği değerlendirildiğinde, kurulacak resmi siber güvenlik biriminin, çoğu saldırıyı erken önleme adına siber caydırıcılığa katkıda bulanacağı değerlendirilmektedir. Siber suçlarla mücadelede yasal zeminin doldurulması, siber suçlara karşı uygulanacak ceza ve yaptırımların açıkca belirtilmesi yine ülke siber caydırıcılığına katkıda bulunacaktır. Yakın gelecekte, olası bir savaşın kendisini, öncelikle siber savaş olarak göstereceği ve konvansiyonel savaşın siber savaş sonrasında gerçekleştirileceği değerlendirilmektedir. Her ne kadar siber ülke güvenliği kaygısı, E-Devletleşme süreci üzerinde bir baskı unsuru olarak bulunsa da teknolojinin insanoğluna ve kamu yönetimine sunduğu yeni imkan ve kabiliyetlerden vazgeçmek veya bu gelişmelerden geri kalmak mümkün görünmemektedir. Alınacak tedbirlerin, çoğu saldırının önüne geçebileceği ve zarar gören sistemin kısa süre içerisinde yine teknolojinin yardımıyla ayağa kaldırılabileceği değerlendirildiğinde, siber güvenlik korkusu, E-Devlet kazanımlarının veya gelişiminin önünde bir engel olmamalıdır. Siber ülke güvenliği, en alt birimden en üst seviyeye kadar alınabilecek önlemler ile sağlanabilmekte veya alınan önlemlerle olası bir siber saldırının, ülke güvenliğine tesiri ve etkisi en aza indirilebilmektedir hipotezi kendisini doğrulamıştır. Alınacak önlemler ve atılacak kararlı adımlarla, siber ülke güvenliği kaygısı ülkeler açısından bir bilinmezlik ve korku kaynağı olmaktan çıkarılmalı, E-Devletleşme sürecine ülke menfaatleri sebebiyle destek verilmelidir.

KAYNAKÇA

Altın, E., "Türkiye'de Elektronik İmza ve Elektronik Devlet Uygulamaları", *Türk Kütüphaneciliği Dergisi,* 2008/22, (3), ss. 280-287.

Akgün, B., (2003), Küreselleşme, Sanal Siyaset ve E-Demokrasi, Küresel Sistemde Siyaset, Yönetim, Ekonomi, Çizgi Kitabevi, Konya.

Aktan, C., M., Tunç, "Bilgi Toplumu ve Türkiye", *Yeni Türkiye Dergisi,* 1998 (Ocak-Şubat), ss. 118-134.

Aktan, C., (2005), Bilgi Çağı Bilgi Yönetimi ve Bilgi Sistemleri, Çizgi Kitapevi, Konya.

Alkan, Mustafa, "Siber Güvenlik ve Siber Savaşlar", *Bilgi Güvenliği Derneği,* <http://www.slideshare.net/Niyazi_SARAL/sber-gvenlk-ve-sber-savalar> 07.01.2014.

Alkan M., A., Atalay, C., Bilirgen, vd. …, "Ulusal Siber Güvenlik Stratejisi", T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *Bilgi Güvenliği Derneği,* <http://www.bilgiguvenligi.org.tr/index_files/pdf/Ulusal_Siber_Guvenlik_Stratejisi.pdf> (07.12.2013).

Alnıak, Oktay, "Siber Terörizm Raporu No: 2", *Türk Asya Stratejik Araştırmalar Merkezi (TASAM),* <http://www.tasam.org/Files/Icerik/File/siber_terorizm_raporu_84be5753-d219-418f-9a68-e6c719b645b1.pdf> (23.12.2014).

Arifoğlu A., vd., (2002) E-Devlet Yolunda Türkiye, Türkiye Bilişim Derneği Yayınları, Ankara.

Baliç, İbrahim, "Bilgi Güvenliğine Giriş", *TÜBİTAK BİLGEM Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi*, <http://www.bilgiguvenligi.gov.tr/veri-gizliligi/bilgi-guvenligine-giris.html> (16.06.2014).

Bakır, Emre, "5.Boyutta Savaş: Siber Savaşlar", *TÜBİTAK BİLGEM Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi*,

<http://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-i.html> (16.11.2012).

Balay, R., "Küreselleşme, Bilgi Toplumu ve Eğitim", *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi,* 2004/37, (2), ss. 61-66.

Balcı A., vd., (2003) Kamu Yönetiminde Çağdaş Yaklaşımlar, Sorunlar, Tartışmalar, Çözüm Önerileri, Modeller, Dünya ve Türkiye Yansımaları (Editoryal), Seçkin Yayıncılık, Ankara.

Barbosa, A., M., Fernandes, H., Diniz, "Rethinking E-Government Performance Assessment From A Citizen Perspective.", *Public Administration*, 2013 (91), ss. 744-745.

Başbakanlık, "Kamu Bilgi Sistemlerinde Birlikte Çalışabilirlik Esasları Rehberi", *T.C. Başbakanlık Genelgesi,* 2005/20.

Baştan, S., R., Gökbunar, "Kamu Hizmetlerinin Sunumunda E-Devletle İlgili Yeni Gelişmeler: Tümleşik E-Devlet Sistemlerine Doğru", *Dokuz Eylül Üniversitesi İ.İ.B.F. Dergisi,* 2004/19, (1), ss. 71-89.

Bekkers, V., "Why does e-government looks as it does? Looking beyond the explanatory emptiness of the e-government concept", *Information Polity: The International Journal of Government & Democracy in the Information Age,* 2012, (17), ss. 329-334.

Bıçakcı, S., "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler Dergisi*, 2012/9, (34), ss. 206-222.

Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, "Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri", <http://www.cybersecurity.gov.tr/publications/uksgf.pdf> 25.02.2013.

Boydak Bilişim Bülteni, Türkiye Siber Ordu Kurmakta Geç Kaldı, <http://www.boydakbilisim.com/2013/02/turkiye-siber-ordu-kurmakta-gec-kaldi> (27.11.2014).

Brunner, Elgin M. ve M., Suter, (2009), An Inventory Of 25 National and 7 International Critical Information Infrastructure Protection Policies, *International CIIP Handbook 2008/2009*, ss. 433-483, <http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf> (02.03.2013).

Btk, (2011), "Ulusal Siber Güvenlik Tatbikatı 2011", *Bilgi Teknolojileri ve İletişim Kurumu*, <http://www.tk.gov.tr/sayfa.php?ID=28> (30.04.2012).

Btk, (2013), "2.Ulusal Siber Güvenlik Tatbikatı Başarıyla Tamamlandı", *Bilgi Teknolojileri ve İletişim Kurumu,* <http://www.tk.gov.tr/sayfa.php?ID=153> (15.09.2013).

Büke, Ahmet, "Bilişim Çağında E-Devlet ve e-Türkiye", *İzmir Ticaret Odası Yayını,* 2002, <http://edevlet.net/eTurkiye/edevlet_ab.pdf> (02.02.2015).

Government of Canada, "Canada's Cyber Security Strategy", <http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf> (05.04.2014).

Cihan Haber Ajansı, "Bakan Yıldırım: Siber Güvenlik Ülke Güvenliğiyle Eş Değer Duruma Geldi", <http://www.cihan.com.tr/caption/Bakan-Yildirim-Siber-guvenlik-ulke-guvenligiyle-es-deger-duruma-geldi-CHODkyMjI0LzE=;jsessionid=E34BE67A240FAE2C06B424308C62E4DF > (01.01.2014).

Cnns, "Ulusal Güvenlik Sistemleri Komitesi Sözlüğü", <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.> (15.08.2012).

Çarıkçı, Oğuzhan, "Türkiye'de E-Devlet Uygulamaları Üzerine Bir Araştırma", *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 2010, (12), ss. 100-101.

Debrah Yaw A. ve I. G., Smith, (2001), "Globalization, employment and the workplace.", Routledge Yayınevi, ss.2-3.

Demir, Ö., (2003), Küresel Rekabette Etkin Devlet, Nobel Yayın Dağıtım, Ankara.

Dpt, (2011), "Bilgi Toplumu İstatistikleri", *Devlet Planlama Teşkilatı Müsteşarlığı, Yayın No: 2826,* <http://www.bilgitoplumu.gov.tr/Documents/1/Diger/Bilgi_Toplumu_Istatistikleri_2011.pdf> (03.09.2014).

Dünya Bankası, (2013), "Ülke ve Yıllara Göre İnternet Kullanım Oranları Yüzdesi", <http://data.worldbank.org/indicator/IT.NET.USER.P2/countr ies/1W-TR-US?display=default> (24.03.2013).

Eken, Hurigül, "Küreselleşme ve Ulus Devlet", *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 2006, (16), ss. 243-262.

Emiroğlu, Bülent Gürsel (2003), E-Devlet: Yapıları Durumu, Sunulan Servisler, Dünyada Gerçekleştirilen Uygulamalar, Türkiye'deki Çalışmalar ve Model Önerisi, <http://www.cyberpark.com.tr/tbd/teknoloji%5CT302.doc> (17.08.2014).

Erdut, Z., (2003), Uluslararası Sosyal Politika ve Türkiye, Dokuz Eylül Yayınları, İzmir.

Erkan, H., (1997), Bilgi Toplumu ve Ekonomik Gelişme, Türkiye İş Bankası Yayınları, Ankara.

Erkan, Hüsnü ve C.Erkan, (1998), Kültür Politikamızda Yeni Boyutlar, TC Kültür Bakanlığı Yayınları, Ankara.

Ernsdorff, M. ve Berbec A. (2007), Estonia: The Short Road to E-government and E-democracy, E-government in Europe, Abingdon, Routledge, ss. 171.

Fedai, R., (2011) *Küreselleşme Sürecinde Kamu Yönetimi: Bürokrasiden Yönetime Değişim,* (Yayımlanmış Yüksek Lisans Tezi), Cumhuriyet Üniversitesi (12.11.2014).

Flaten, R. Drolsum ve Soysa Indra, "Globalization and Political Violence.", *International Interactions,* 2012, (38), ss. 626-629.

Gelinas, R. R., (2010), Cyberdeterrence and The Problem of Attribution, Georgetown Üniversitesi Bilim ve Sanat Fakültesi, Washington.

Geray, H., (2004), Toplumsal Araştırmalarda Nicel ve Nitel Yöntemlere Giriş, Siyasal Kitapevi, Ankara.

Glennon, Michael J., "State-Level Cybersecurity", *Policy Review Dergisi*, 2012, (171), ss. 88.

Gökçe, A.Gençer, "Bilgi Güvenliği Farkındalığı Nasıl Ölçülür?", *TÜBİTAK BİLGEM Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi*, 2010, <http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-farkindaligi-nasil-olculur-1.html> (16.11.2013).

Güçlü, Mustafa, "Küreselleşmenin Tarihi Seyri", *Türkiye Günlüğü Dergisi,* 2006, (86).

Gültekin, B., (2007) *Türkiye'de E-Devlet uygulamaları ve Toplumsal Açılımları*, (Yayımlanmış Yüksek Lisans Tezi), Gazi Üniversitesi, (15.08.2013).

Halchin, L.Elaine, "Electronic Government: Government Capability and Terrorist Resource", *Government Information Quarterly Dergisi*, 2004, (21), ss. 406-419.

Henrie, Morgan, "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment.", *Engineering Management Journal*, 2013, (25), ss. 38-40.

Hodoş, Raul Felix, "Computerization Of Public Administration To Egovernment: Between Goal And Reality", *Juridical Current,* 2014, (17), ss. 120.

Hub, Miloslav, "Security Evaluation of Passwords Used on Internet", *Journal of Algorithms & Computational Technology*, 2011/5, (3), ss. 437-440.

Ionescu, Luminata, "The Role Of E-Government In Curbing The Corruption In Public Administration", *Economics, Management, and Financial Markets,* 2015, (10), ss. 48-53.

Itu, (2008), "Veri Ağları, Açık Sistem Haberleşmeleri ve Güvenlik Raporu", *Uluslararası Telekomünikasyon Birliği,* No.X.1205, <http://www.itu.int> (15.10.2013).

Itu, (2011), "Ulusal Siber Güvenlik Strateji Rehberi", *Uluslararası Telekomünikasyon Birliği,* ss. 5, <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU NationalCybersecurityStrategyGuide.pdf> (12.01.2014).

Itu, (2011), "Siber Güvenlik, Online Dünyayı Daha Güvenli Yapmak", *Uluslararası Telekomünikasyon Birliği,* <http://www.itu.int/net/itunews/issues/2011 /05/38.aspx> (15.06.2013).

İçişleri Bakanlığı, "E-Dönüşüm Araştırması Raporu", *İçişleri Bakanlığı Araştırma ve Etütler Merkezi,* 2004, Ankara, <www.arem.gov.tr> (15.09.2013).

İnce, M, (2001), Elektronik Devlet: Kamu Hizmetlerinin Sunulmasında Yeni İmkânlar, DPT Yayınları, Ankara.

İto, (2003), E-Devlet Uygulamaları ve Ekonomiye Etkileri, *İstanbul Ticaret Odası,* Acar Matbaacılık, İstanbul.

Kenyon, S. Henry, "Cyber Attacks Reveal Lessons", *SIGNAL Magazine*, 2009/07, ss. 10-12, <http://usacac.army.mil/cac2/call/docs/10-12/ch_7.asp> (25.03.2013).

Keyman, Fuat, "Globalleşme Söylemleri ve Kimlik Talepleri: Türban Sorununu Anlamak.", *Düşünen Siyaset*, 1999, (3), ss. 71–90.

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

Levi, Albert, "Nasıl Bir E-posta Güvenligi?", *Sabancı Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi,* 2012, <http://people.sabanciuniv.edu/levi/bilisim guvenlik1.pdf> (15.10.2012).

Lewis, James.A., "Cybersecurity and Critical Infrastructure Protection", *Center for Strategic and International Studies,* 2006, <http://cip.management.dal. ca/publications/Cybersecurity%20and%20Critical%20Infrastructure%20 Protection.pdf> (04.03.2014).

Lin, Harbert, "A Virtual Necessity: Some Modest Steps Toward Greater Cybersecurity", *Atomic Scientists Dergisi*, 2012, (68), ss. 75-87.

Loo, Alfred, "The Myths And Truths of Wireless Security", *Communications of the ACM Dergisi*, 2008/2, (51), ss. 66-71.

Malhotra, Y., (1997), Knowledge Management in Inquiring Organizations. Proceedings of 3rd Americas Conference on Information Systems. Indianapolis, ss. 239-295.

Meinhard, Stephanie ve P., Niklas, "The Globalization-Welfare State Nexus Reconsidered.", *Review of International Economics*, 2012, (20), ss. 271-273.

Mellouli, Sehl, "Ingredients for the Success of an E-Government Website", *The American Society for Public Administratio,* (Edt. Sonia M. Ospina ve Rogan Kersh), 2014/2, (74), ss. 283-285.

Menteş, Erinç Ali, "Devletin Evrim Sürecinde Yeni Bir Aşama: E-Devlet", 2003, <http://dergi.emo.org.tr/altindex.php?sayi=417&yazi=49> (20.01.2015).

Miles, Ian, "Transformations of Information Society", 2004, <http://www.eolss.net/sample-chapters/c13/E1-24-01-04.pdf> (05.05.2015).

Mihalache, Adrian, "The Cyber Space–Time Continuum: Meaning and Metaphor", *Information Society*, 2002, (18), ss. 293-300.

Milliemlak, "E-Devlet", 2003, <http://www.milliemlak.gov.tr/e_devlet/e_devlet.htm> (17.08.2013).

Milliyet Gazetesi, "70 Milyonun Bilgilerini Sattılar", Hasan Örnekoğlu, 28.07.2010.

Murshed, S.Mansoob, "Perspectives on two phases of globalization.", *Globalization, Marginalization & Development,* 2002, ss. 1-3.

Mutioğlu, Halil, "Küreselleşme ve E-(tik) Devlet", *I. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi, K.Ü. İ.İ.B.F. Yayını,* 2002, İzmit, ss. 957-964.

The New York Times, "State's Secrets: Leaked Cables Offer Raw Look at U.S. Diplomacy", Scott Shane, (29.11.2010), <http://www.nytimes.com/2010/11/29/world/29cables.html?pagewanted=1&_r=3> (07.09.2014).

Önal, Huzeyfe, "Siber Saldırı Aracı Olarak DDoS", *Bilgi Güvenliği Akademisi,* 2013, <http://www.bga.com.tr/calismalar/siber_savas_ddos.pdf> (06.02.2013).

Pras, A., A.,Sperotto, G., Moura, vd. …, "Attacks by "Anonymous" WikiLeaks Proponents not Anonymous", *Hollanda Twente Üniversitesi Teknik Raporu,* 2010, <http://eprints.eemcs.utwente.nl/19151/01/2010-12-CTIT-TR.pdf> (15.11.2014).

Pudelko M., C., Carr, J., Henley, "Globalization and Its Effects on International Strategy and Cross-Cultural Management.", *International Studies of Management & Organization,* 2006, (36), ss. 4-5.

Radikal Gazetesi, "YÖK'ten Siber Saldırıya Suç Duyurusu", (10.01.2013) <http://www.radikal.com.tr/turkiye/yokten_siber_saldiriya_suc_duyurusu-1116290>

Rukancı, Fatih ve H., Anameriç, "Bilgi Toplumu ve Toplumun Bilgilenmesine Kütüphanelerin Rolü", *Kütüphaneciliğin Destanı Uluslararası Sempozyumu Bildiriler,* 2004, <http://acikarsiv.ankara.edu.tr/fulltext/165.htm> (02.05.2013).

Saalbach, Klaus, "Siber Savaş Yöntemleri ve Uygulamaları", *Osnabrück Üniversitesi Yayınları,* 2013, ss. 11.

Sabah Gazetesi, "Anonymous BTK'yı da hackledi", 14.02.2012, <http://www.sabah.com.tr/teknoloji/2012/02/14/anonymous-btkyi-da-hackledi>

Sağıroğlu, Şeref, "Siber Bilgi Güvenliği ve Savunma Yöntemleri", Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, 2013, <http://ceng.gazi.edu.tr/~guvenlik/BBG5.pdf>, (07.01.2013).

"Sanal Tehdit Bilgisayar Virüsleri", *Bilim ve Teknik Dergisi,* Mayıs 2005, ss. 3-4.

Saraçbaşı, Y., (2010), "*Türkiye'de E-Belediyecilik Uygulamalarında Belediye Vatandaş İlişkisi: Malatya Belediyesi Örneği*", (Yayımlanmış Yüksek Lisans Tezi), Süleyman Demirel Üniversitesi Sosyal Bölümler Enstirüsü Kamu Yönetimi Anabilim Dalı, <eprints.sdu.edu.tr/760/1/ TS00824.pdf> (15.01.2014).

Shishkov, Y.V., (2014), Information Revolution, Value Inquiry Book Series, ss. 273-274.

"Siber Güvenlik Çalıştayı Yapıldı", *Bilişim Ajandası Aylık Bilişim Kültürü Dergisi,* 2011, (136), ss. 20-23.

Sterner, E., "Wikileaks and Cyberspace Cultures in Conflict", *The George C. Marshall Policy Outlook,* 2011.

Şahin, Ali ve E.Örselli, "E-Devlet Anlayışı Sürecinde Türkiye", *Sosyal Bilimler Enstitüsü Dergisi,* 2003, ss. 346.

Şahinaslan E., A. Kantürk, Ö., Şahinaslan, E., Borandağ, "Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri", *Harran Üniversitesi Akademik Bilişim Konferansı Bildirileri,* 2009, ss. 597-602, <http://ab.org.tr/ab09/kitap/sahinaslan_kanturk_AB09.pdf> (05.01.2015).

Tekman, E., (2002), Enformatik Sistemler ve Bilgi Toplumu, Bilgi Toplumuna Geçiş, (Edt. İlhan Tekeli ve Diğerleri), Türkiye Bilimler Akademisi Yayınları, Ankara.

Tonta, Yaşar ve M.E., Küçük, "Sanayi Toplumundan Bilgi Toplumuna Geçiş Sürecinde Temel Dinamikler", Genelkurmay Başkanlığı Bilgi Çağı ve Teknolojik Gelişmeler Işığında Toplum, Yönetim, Yönetici ve Lider Yaklaşımları Uluslararası Sempozyumu, 2005, İstanbul, ss. 8.

Torun, İshak (2003), "Endüstri Toplumunun Oluşmasında Etkili Olan İktisadi ve Sina-İ Faktörler", *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi,* 2003/4, (1), ss. 181-194.

Tsk, "21 Ocak 2013 Tarihli Basın Açıklaması", Türk Silahlı Kuvvetlerinden Haberler, 2013, <http://www.tsk.tr/3_basin_yayin_faaliyetleri/3_4_tsk_haberler/2013/tsk_haberler_06.html> (22.01.2013).

Tuik, "Hane Halkı Bilişim Teknolojileri Kullanım Araştırması", T.C. Türkiye İstatistik Kurumu Başkanlığı, 2012, <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10880> (06.02.2012).

Tunaya, T.Z., (1980), Siyasal Kutrumlar ve Anayasa Hukuku, 4. Basım, İstanbul Üniversitesi Hukuk Fakültesi Yayınları, İstanbul.

Turgut, Arzu, "Wikileaks Belgelerinde Türkiye ve Yakın Çevresi", *Uluslararası Stratejik Araştırmalar Kurumu USAK Raporu*, 2011/11, ss. 9.

Türk Dil Kurumu, "Büyük Türkçe Sözlük", <http://www.tdkterim.gov.tr/bts> (20.12.2012).

Türkiye Bilişim Derneği, "E-Belediye Taslak Rapor (I), Türkiye Bilişim İkinci Şurası", Ankara, <http://www.bilisimsurasi.org.tr/e-turkiye/docs/e-belediye-taslakraporu-1-5.doc> (20.12.2013).

Uçkan, Özgür, "E-Devlet, E-Demokrasi ve E-Yönetişim Modeli: Bir İlkesel Öncelik Olarak Bilgiye Erişim Özgürlüğü", 2003, <http://www.stradigma.com/turkce/haziran2003/makale_09.html> (23.12.2014).

Ulusoy, Ahmet ve K., Birol, "Türkiye'nin E-Devlete Geçiş Zorunluluğu", I. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi, K.Ü. İ.İ.B.F. Yayını, 2002, İzmit, ss. 131-144.

Unctad, "Information Economy Report", United Nations Conference on Trade and Development, Geneva, 2005, ss. 187.

Ülker, Halil İ. (2002), "Bilgi Toplumu ve Devlet", 1. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi Bildiriler Kitabı, 10-11 Mayıs 2002, Kocaeli, ss. 949-956.

Vukasinovic, Jelena, "Role Of Knowledge In Informatıon Society", Singidunum Journal of Applied Sciences, 2014, ss. 476-478.

Yeni Şafak Gazetesi, "5 Bin MİT Ajanı Deşifre Mi Oldu?", (14.08.2007), <http://beta.yenisafak.com.tr/gundem-haber/5-bin-mit-ajani-desifre-mi-oldu-14.08.2007-62068> 20.05.2014.

Yeni Şafak Gazetesi, "Öğretmenin Kimliği Çalındı", Yakup Bulut, (13.02.2014).

Yılmaz, Kürşad ve M.B., Horzum, "Küreselleşme, Bilgi Teknolojileri ve Üniversite", *İnönü Üniversitesi Eğitim Fakültesi Dergisi,* 2005/6, (10), ss. 103-121.

Wikipedia, Özgür Ansiklopedi, 2013, <http://en.wikipedia.org> (23.03.2013).

White House, "Kapsamlı Ulusal Siber Güvenlik Girişimi", *ABD Beyaz Saray Başkanlığı,* 2012, <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf> (24.10.2012).

White House, "ABD Beyaz Saray Basın Açıklaması", Başkanın Ulusun Siber Altyapısı ile İlgili Konuşmaları, 2009, < http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure> (13.01.2013).

Weimann, Gabriel, "Siber Terörizm, Tehlike ne kadar gerçek?", Amerika Birleşik Devletleri Barış Enstitüsü Özel Raporu, 2004, <http://dspace.cigilibrary.org/jspui/bitstream/123456789/15033/1/Cyberterrorism%20How%20Real%20Is%20the%20Threat.pdf?1> (27.01.2013).