

Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması

Köksal ÖZENÇ

Özet-Günümüzün gelişen teknolojisi nedeniyle bilgi ve verilerin güvenliğine olası riskler de dolayısı ile doğru orantılı olarak artmaktadır. İnternet güvenliği konusundaki yazılımlara ilişkin pazarın 1999 yılı sonu itibari ile yaklaşık 4,4 milyar ABD Doları olduğu, bu rakamın yılda ortalama %23'lük bir artış ile 2004 yılında 8,3 milyar ABD Doları'na ulaşabildiği ifade edilmektedir. Diğer taraftan AB'inde de önemli bir yer teşkil eden bilgi ve iletişim teknolojilerindeki bilgi güvenliği konusunda yapılan harcamaların 2000 yılında 465 milyon ABD Doları iken bu rakam 2006 yılında 2,74 milyar ABD Dolar gibi oldukça büyük bir meblağa ulaşmıştır. Zira AB'nin toplam bütçesi 5,3 milyar Euro olan 7. Çerçeve Programı çerçevesinde bilgi güvenliğine ilişkin teknolojiler hususunda yapılacak araştırma projelerine 2007/2013 dönemi içinde oldukça büyük bir miktar olarak 1,4 milyar Euro'luk bir bütçe ayrılmıştır [1].

Anahtar Kelimeler-Bilgi güvenliği, bilgisayar, güvenlik

Abstract-And the risks against the security of the information and data because of our today's developing technology increase too. The certain sources say that the market on the software programs for the internet security was about USD 4,4 bn as for the last of 1999 and also this figure amounts to USD 8,3 bn with an increase of % 23 on average per year. Furthermore while the overheads done for information security in the information and communication technologies which has great importance for EU were USD 465 million, this amount increased up to USD 2,74 bn in 2006. Because Euro 1,4 bn in the term of 2007/2013 has been assigned for the R&D projects in the field of information security technologies within the context of the 7th Framework Program which has a budget of Euro 5,3 bn [1].

Index Terms-Information security, computer, security

I. GİRİŞ

Günümüzde, gelişmiş ülkelerde başta olmak üzere, bilgi toplumu olma yolunda hızlı bir değişim süreci yaşanmaktadır. Bu süreçte etkin rol oynayan bilgi ve

Köksal ÖZENÇ, Telekomünikasyon Uzmanı, Telekomünikasyon Kurumu, Ankara, kozenc@tk.gov.tr

iletişim teknolojileri, iletişim, elektronik bankacılık, elektronik imza, uzaktan eğitim, kamu hizmetleri ve e-devlet uygulamaları gibi pek çok alanda yer alarak günlük yaşamı bütünüyle değiştirmeye başlamıştır.

Bilgi toplumu hedefine ulaşılması ve elektronik imzaya dayalı elektronik devlet ve elektronik ticaret uygulamalarının yaygınlaşması için büyük önem taşıyan bilgi ve iletişim teknolojilerinde güvenli bir ortamın, açık ağlarda dolaşan bilginin güvenliğinin ve kişisel verilerin gizliliğinin sağlanması ile mümkün olmaktadır. Bu nedenle, taraflararası iletilerde bilginin gizliliği, bütünlüğü ve her istenilen anda erişilebilirliğinin sağlanması için teknik ve hukuki önlemlerin alınması büyük önem arz etmektedir.

Çok çeşitli sayıda bilgi ve iletişim teknolojilerinin günümüzde hızla artan bir oranda kullanılır hale gelmesi ekonomik ve sosyal hayatta karşılaşılan pek çok işlemleri kolaylaştırdığı ölçüde bilgi güvenliğine karşı çeşitli boyutlarda risk ve tehditleri de beraberinde getirebilmektedir. Zira yabancı ülkelerde olduğu gibi ülkemizde de bilgisayar ve mobil iletişim teknoloji ve cihazlarının her geçen gün artan bir şekilde kullanılır hale gelmesi ve bu teknoloji ve sistemleri kullanan kişilerin de büyük bir çoğunlukla bilgi güvenliğine karşı oluşabilecek risk ve tehditlerin farkında değildirler. Oluşan bu risk ve tehditler, kişilerin çoğunlukla maddi kayba uğramalarına ya da bilgilerinin değiştirilmesi, silinmesi ya da izinsiz olarak erişilmesi gibi istenmeyen bazı durumlara neden olabilmektedir.

II. BİLGİ VE İLETİŞİM TEKNOLOJİLERİNDEKİ BİLGİ GÜVENLİĞİNİN EKONOMİK BOYUTU

Günümüzün gelişen teknolojisi nedeniyle bilgi ve verilerin güvenliğine olası riskler de dolayısı ile doğru orantılı olarak artmaktadır. İnternet güvenliği konusundaki yazılımlara ilişkin pazarın 1999 yılı sonu itibari ile yaklaşık 4,4 milyar ABD Doları olduğu bu rakamın yılda ortalama % 23'lük bir artış ile 2004 yılında 8,3 milyar ABD Doları'na ulaşabileceği yönünde bir tahmin yapılmaktadır. Diğer taraftan AB'inde de önemli bir yer teşkil eden bilgi ve iletişim teknolojilerindeki veri güvenliği konusunda yapılan harcamaların 2000 yılında 465 milyon ABD Doları iken

bu rakamın 2006 yılında 2.74 milyar ABD Doları ulaşabilecektir. Zira AB'nin toplam bütçesi 5,3 milyar Euro olan 7. Çerçeve Araştırma Programı çerçevesinde veri güvenliğine ilişkin teknolojiler hususunda yapılacak araştırma projelerine 2007/2013 dönemi için oldukça büyük bir meblağ olarak 1,4 milyar Euro'luk bütçe ayrılmıştır.

1995 yılında sadece 20.000 olan web sitesinin sayısı, 1997 yılında 700.000'e ve 2002 yılında ise 37 milyona ulaştığı dikkate alındığında internet ve multimedya ortamında kullanılan ses, data ve görüntü olmak üzere her türlü bilgi ve verinin güvenlik boyutunun ne kadar önemli olduğu ve buna bağlı olarak da güvenliğin sağlanması sorununun çözülmesinin de bir o kadar karmaşık ve zor olduğu ortaya çıkmaktadır.

Ayrıca bilgi ve iletişim teknolojilerinin özelliği nedeniyle veri güvenliği hususunda uluslararası işbirliği de çok önemlidir. Zira günümüzün gelişen teknolojisi sayesinde bilişim suçları artık sınırları aşan bir boyut kazanmıştır. Örneğin, 2000 yılında ortaya çıkan Love Letter virüsünün tüm dünyada yaklaşık 7 milyar ABD Doları zarar verdiği tahmin edilmektedir.

Benzer şekilde 2001 yılında Code Red Worm virüsü ortaya çıktığından itibaren ilk 14 saat içinde 359.000 adet sisteme zarar verirken, 2003 yılında ortaya çıkan Sequel Slammer virüsü ise bundan çok daha hızlı bir şekilde yayılma göstererek sadece ilk 10 dakika içinde 75.000 adet sisteme zarar verdiği tahmin edilmektedir.

FBI tarafından yapılan araştırmaya göre halen günümüze kadar yaklaşık 70.000 adet virüsün tesbit edildiği ve dünyada mevcut olan internet web server'lerinin yaklaşık %85'inin en az bir kez siber saldırıya maruz kaldığı dikkate alındığında konunun ekonomik boyutunun olduğu kadar uluslararası ilişkiler boyutunun da ne kadar önemli olduğu ortaya çıkmaktadır.

Yukarıda belirtilen rakamlardan da anlaşılacağı üzere bilgi ve iletişim teknolojilerindeki bilgi güvenliğine ve kişisel mahremiyete gerek yazılım gerekse de donanım açısından çok büyük yatırım ve harcama yapılmaktadır. Bu da hem bireysel kullanıcılara ve hem de kurumsal maddi külfet getirmektedir.

III. BİLGİ GÜVENLİĞİNDE AB'NİN HUKUKİ YAKLAŞIMI

Yukarıda belirtilen hususlar çerçevesinde istenmeyen bu durumların engellenebilmesini teminen AB, hukuki alanda aşağıda belirtildiği üzere bazı düzenlemeler yapmıştır [2].

Avrupa Birliği'ndeki bilgi güvenliği alanındaki çalışmalar esas itibarıyla 1987 yılında başlamıştır. 1987 yılında yayınlanan Green Paper (Yeşil Rapor) ile AB, telekomünikasyon sektöründeki bilgi güvenliğinin önemine işaret etmiştir. Ayrıca AB, bilgi ve iletişim teknolojileri üzerinde bilgi güvenliğinin sağlanması ve mahremiyetin korunması konusunda gelişen teknolojik

ve sosyal ihtiyaçları da dikkate alarak telekomünikasyon sektöründe serbestleşmenin Topluluk içinde 2000 yılına kadar tamamlanmasının hedeflendiği 1998 mevzuatı çerçevesinde, aşağıda belirtilen mevzuatı düzenleyerek yürürlüğe koymuştur:

--Kişisel verilerin işlenmesi ve bu bilgilerin serbestçe dolaşımı hususunda bireylerin korunmasına ilişkin 95/46/EC sayılı AB Direktifi (AB mevzuat uyum çalışmaları çerçevesinde söz konusu Direktifin uyumlaştırılması amacıyla Adalet Bakanlığı tarafından taslak bir yasa çalışması halen devam etmektedir.)

--Telekomünikasyon sektöründeki kişisel verilerin işlenmesi ve mahremiyetin korunmasına ilişkin 97/66/EC sayılı AB Direktifi

Diğer taraftan AB, özellikle 1995'li yıllardan itibaren internet ve multimedya teknolojilerinin toplum tarafından çok büyük bir hızla kullanılır hale gelmesiyle birlikte özellikle internet teknolojilerinin beraberinde getirdiği bazı kolaylıklar ve imkanlara ilaveten küçük çocukların internet ortamındaki müzır yayınlardan korunması amacıyla "Küresel ağlar üzerinde zararlı ve yasadışı içerikle mücadeleyle internetin daha güvenli kullanımı" hususunda 99/276/EC sayılı bir Karar yayınlamıştır.

Ayrıca, 1998 tarihli mevzuat çerçevesinde telekomünikasyon sektöründe hedeflenen serbestleşmeyi tamamlayan AB, bu kez teknolojideki ve buna bağlı olarak da telekomünikasyon sektöründe

- * ses ve veri
- * telekomünikasyon ve radyo-TV yayını
- * sabit ve mobil

hizmetler olmak üzere üç farklı alanda gerçekleştirilen ve toplum hayatını ve dolayısı ile de telekomünikasyon alanındaki düzenlemeleri derinden etkileyen yakınsama konusunu dikkate alarak 2002 tarihinde yeni bir düzenleyici çerçeve mevzuatını hazırlayarak yürürlüğe koymuştur.

Yukarıda belirtilen hususlar çerçevesinde telekomünikasyon, radyo-TV yayını, sabit ve mobil hizmetler, ses ve veri hizmetleri, internet ve multimedya hizmetlerindeki bu yakınsama nedeniyle artık AB, 1998 tarihli çerçeve mevzuatında yer alan ve teknolojiye bağlı olan diğer bir deyişle belirli bir teknolojiye çağrıştıran "telekomünikasyon", radyo-TV yayıncılığı", "uydu hizmetleri", "sabit ses hizmetleri", "mobil hizmetler", "veri hizmetleri" gibi tanım ve ifadeler yerine tüm bunları tek bir başlık altında kapsayacak şekilde ve teknoloji nôtür bir ifade olan dolayısı ile de teknolojilerin her alanında yakınsamayı ifade eden "elektronik haberleşme şebekeleri ve hizmetleri" şeklinde farklı bir tanımla gündeme getirmiştir.

Bu kapsamda, 2002 yılında kabul edilen ve 2003 yılında AB üyesi ülkelerde yürürlüğe giren yeni çerçeve düzenleyici paket kapsamında 1998 tarihli mevzuatta yer alan telekomünikasyon sektöründeki kişisel verilerin işlenmesi ve mahremiyetin korunması konusundaki 97/66/EC sayılı AB Direktifi'nin yerine geçen elektronik haberleşme sektöründe mahremiyetin

korunması ve kişisel verilerin işlenmesi hususundaki 2002/58/EC sayılı Direktifi yürürlüğe koymuştur. AB mevzuat uyum çalışmaları çerçevesinde sözkonusu Direktifin uyumlaştırılması amacıyla Kurum tarafından 06.02.2004 tarihinde Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik çıkartılmıştır.

Yukarıda belirtilen hususların yanı sıra, AB yukarıda sayılan direktifleri tamamlayıcı nitelikte olmak üzere aşağıda belirtilen bazı kararlar almıştır.

--Bilgi güvenliğinin sağlanmasına ilişkin 31 Mart 1992 tarih ve 92/242/EC sayılı Konsey Kararı,

--Şebeke ve bilgi güvenliği kültürüne doğru Avrupa'nın yaklaşımına ilişkin 18 Şubat 2003 tarih ve 2003/48/EC sayılı Konsey Kararı,

--Şebeke ve bilgi güvenliğinin iyileştirilmesi ve uygulamanın yayılması ile ilgili e-Avrupa Eylem Planı'nın izlenmesine ilişkin 17 Kasım 2003 tarih ve 2256/2003/EC sayılı Konsey Kararı,

Ayrıca, yukarıda belirtildiği üzere kişisel verilerin ve mahremiyetin korunmasına yönelik olarak bir çok farklı alanda düzenleme yapma ihtiyacı hisseden AB, sözkonusu düzenlemelerden özellikle genel anlamda ve sektör spesifik alanda olmak üzere iki ayrı yapı halinde kurumsallaşmaya doğru da bir adım atmıştır. Bu çerçevede kişisel verilerin ve mahremiyetin korunmasına yönelik olarak 95/46/EC sayılı Direktifte belirtilen hususlara kurumsal bir yapı kazandırmak amacıyla "Topluluk kurumları tarafından kişisel verilerin işlenmesi, kişilerin korunması ve bilgilerin serbest dolaşımı"na ilişkin olarak onayladığı 2001/45/EC sayılı Tüzük ile AB içinde ilk kez "Veri Koruma Görevlisi" ve "Avrupa Veri Koruma Denetmeni" gibi bazı görev ve fonksiyonlara işlerlik kazandırılmıştır.

Benzer şekilde sektör spesifik bir alanda, sadece telekomünikasyon sektörüne özgü olmak üzere ve bu kapsamda düzenleme amacıyla yürürlüğe konulan 2002 tarihli yeni düzenleyici çerçeve mevzuatı kapsamında kabul edilen elektronik haberleşme şebeke ve hizmetleri konusundaki 2002/58/EC sayılı Direktif ve 99/276/EC sayılı Karar'a ilişkin hükümleri de kapsayacak şekilde AB tarafından "Avrupa Şebeke ve Bilgi Güvenliği Kurumu"nun (ENISA-European Network and Information Security Agency) kurulması amacıyla 2004/460/EC sayılı Tüzük yayınlanmıştır.

Yukarıda belirtilen hususlara ilaveten AB, özellikle tüm dünyada 1990'lı yıllardan itibaren gelişen ve yaygınlaşan elektronik ticaret ve elektronik imza uygulamalarına özgü çıkartmış olduğu 2000/31/EC ve 99/93/EC sayılı Direktifler'de de kişisel verilerin ve mahremiyetin korunmasını sağlamak üzere kriptografi ve elektronik imza teknolojileri çerçevesinde uygulanan standartlara ilişkin olarak bazı hükümler getirmiştir.

Son olarak da AB tarafından elektronik haberleşme şebekeleri kullanılarak gerçekleştirilen tüm haberleşmenin (telefon, faks, VoIP, e-posta vs.) kim tarafından ne zaman ve kimle yapıldığına dair ve

haberleşmenin içeriği de dahil olmak üzere ileride meydana gelebilecek herhangi bir yasal soruşturma ya da incelemede kullanılabilmesini teminen gerekli olabilecek tüm bilgilerin 6 aydan az olmamak ve 2 yıldan fazla olmamak şartıyla depolanması yönünde telekomünikasyon sektöründeki mobil işletmecilere, sabit işletmecilere, MVNO ve ISP gibi diğer tüm sektör aktörlerine bir görev verilmiştir. Bu çerçevede 13.4.2006 tarihli AB Resmi Gazetesi'nde yayınlanan 2006/24/EC sayılı Direktif gereğince bu husus yasal bir zorunluluk haline getirilmiştir.

IV. AB'DE GÜVENLİK KÜLTÜRÜNE İLİŞKİN POLİTİKANIN GELİŞTİRİLMESİ

Bilgi toplumu hizmetlerinin gelişmesiyle bilgi güvenliği, iş dünyasının vatandaşın ve kamu sektörünün yaptığı her işlemde vazgeçilmez bir unsur olmuştur. Bu nedenle, AB bünyesinde ortak tutum, fikir ve anlayış birliğinin kurulması ve iç pazarın sağlıklı çalışması amacıyla, AB içinde güvenlik kültürü oluşturulması hedeflenmiştir. Bu kapsamda, 92/242/EC sayılı Konsey Kararı ile 2002 yılı e-Avrupa Eylem Planı ve 2256/2003/EC ve 2003/48/EC Sayılı Konsey Kararları ile 2005 yılı e-Avrupa Eylem Planları oluşturulmuştur. Bu eylem planlarında;

-- Elektronik ortamda depolanan, işlenen ve iletilen bilginin kazara veya kasıtlı tehditlere karşı uygun şekilde korunması,

--Konu ile ilgili uluslararası standartların kabul edilmesi,

--Konu ile ilgili üye devletlerde gerekli düzenlemelerin yapılmasının gerekliliği,

--Bilgi sistemlerinin güvenliği için kullanıcı ve servis sağlayıcılara düşen görevlerin tanımlanması,

--Her kesimden kullanıcının bilgilendirilmesi ve bilinçlendirilmesi için bilgi ve veri güvenliği ile mahremiyetin korunması eğitimlerine önem verilmesi,

--Özel sektör, Ar-Ge kuruluşları ve hükümetlerin işbirliği içinde olması,

--Bilgi güvenliği ile mahremiyet ihlallerini asgari seviyede tutmak için hukuki, teknik ve idari tedbirlerin alınması,

--Bilişim suçlarının çoğunlukla uluslararası alanda işlenmesi ve sınır tanımaması nedeniyle uluslararası işbirliğine önem verilmesi gerektiği vurgulanmıştır.

V. AB'DEN BİR ÖRNEK: İNGİLTERE

İngiltere, biyometrik güvenlik önlemlerini de içeren kimlik kartlarının vatandaşlara dağıtılması için bir proje başlatmıştır. Zira kimlik bilgilerinin çalınarak kopyalanması sonucu çok sayıda insan maddi ve manevi zarara uğramış bulunmaktadır. İngiltere'de kimlik bilgilerinin çalınmasına karşı mücadele vermek

üzere sivil toplum kuruluşu sıfatıyla kurulmuş olan Cifas'a göre örneğin sadece 2004 yılında 119.000 kişinin kimlik bilgileri kullanılarak maddi çıkar sağlanmıştır. Cifas, İngiltere'de 240 üyesi ile beraber başta telekomünikasyon şirketleri olmak üzere bankacılık sektörü ve çeşitli ticari firmalardaki kişisel bilgilerin başka amaçlarla kullanılmasını önlemek ve kullanıldığı takdirde bunu yetkili makamlara ihbar etmek üzere kar amacı gütmeyen çalışma yapan çok sayıda sivil toplum kuruluşundan birisidir [3].

VI. ULUSLARARASI ARENADA BİLGİ GÜVENLİĞİNE İLİŞKİN BAZI ÖRNEKLER

A. Estonya'ya Siber Saldırı

Mayıs 2007'de Baltık cumhuriyetlerinden Estonya tarafından yaklaşık üç hafta süreyle siber saldırı altında olduğu duyuruldu.

Estonya Hükümeti tarafından yapılan açıklamada devlet kurumlarıyla birçok özel işletmenin internet sitelerini çökerten bu saldırıdan Rusya sorumlu tutulmuş zira hükümet, bu saldırıların, başkent Tallin'deki tartışmalı savaş anıtının kaldırılmasından sonra başladığını ifade etmiştir.

Moskova tarafından yapılan açıklamada ise, anıtın kaldırılmasını Estonya'yı Nazi işgalinden kurtarmaya çalışırken ölen Sovyet askerlerine hakaret olarak yorumlanmıştır.

Anıt, aylar süren tartışmalar ardından 27 Nisan 2007'de kaldırılmış ve Moskova-Tallin ilişkileri gerilmiştir. Kızıl Ordu anıtının kaldırılmasından sonra Rus azınlığın protesto gösterileri sırasında bir kişi ölmüş, 100 kişi yaralanmış, 1300 kişi de tutuklanmıştı. Estonya Hükümeti, internet sitelerine yönelik saldırıların anıtın kaldırılmasının hemen ertesinde başladığını ifade etmiştir.

Siber saldırıda, Estonya Cumhurbaşkanlığı, parlamento, birçok bakanlık siyasi partiler ve bankalarla diğer işletmelerin internet sitelerinin hedef alındığı, aşırı yüklenme nedeniyle ana işlemcilerin çöktüğü ve ülkenin dış dünyayla bağlantısı kesilmiştir. Estonya Savunma Bakanlığı tarafından yapılan açıklamada, saldırının farklı ülkelerden yönlendirildiğini ancak bazılarının Rus devletine ait ana bilgisayarlardan yönlendirildiği ifade edilmiştir.

Estonya, sorumluların bulunabilmesi için NATO, Avrupa Birliği ve ENISA gibi bazı mercilerin uzmanlarından yardım talep etmiştir [4].

B. Carnivore

Carnivore, ABD'de FBI tarafından 2000'li yılların başında geliştirilen özel bir elektronik izleme sistemine verilen isimdir. Bu sistem FBI tarafından daha önceden kullanılan Omnivore adlı sistemin geliştirilmiş versiyonudur. Carnivore sistemi, adli mercilerin izni ile internet üzerinden gerçekleştirilebilecek suçları ve suçluları önleme ve izleme amacıyla ya internet servis

sağlayıcısına bağlanır. Bu sayede takibe alınan kişinin e-posta mesajları, ICQ mesajlaşmaları ve hangi web sayfasında ne kadar süre gezindiği ve ne yaptığı gibi her türlü işlem dahil olmak üzere internet vasıtasıyla gerçekleştirmiş olduğu her türlü işlem takibe alınır. Carnivore sisteminin FBI tarafından kullanılması sayesinde 25600 suçlu yakalanmıştır.

11 Eylül 2001'de ABD'de yaşanan terörist saldırısında iki adet gökdelenin çökmesi sonucu ABD Temsilciler Meclisi tarafından 24 Ekim 2001 tarihinde kabul edilen ABD Vatandaşlık Kanunu ile internetteki her türlü verilerin FBI tarafından izlenmesi ve kayıt altına alınması hüküm altına alınmıştır. Bu çerçevede muhtemel suçluların ve yasal merciler tarafından takip edilen kişilerin internet vasıtasıyla yaptıkları her türlü iletişimin FBI tarafından ISP'lerin sistemlerine ilave edilecek olan Carnivore adındaki bir sistem tarafından izlenmesi ve kayıt altına alınması sağlanmıştır.

Carnivore, hedef bir kişinin ya da kuruluşun internet trafiği dahil olmak üzere tüm haberleşme trafiğinin takip edilmek üzere FBI tarafından kullanılan bir sistem olup, FBI tarafından Omnivore adında kullanılan sistemin daha gelişmiş halidir. Omnivore sistemi Şubat 1997'de kullanılmaya başlanmış ancak bilahare FBI tarafından daha da geliştirilerek kod adı "DCS1000" (DCS - Digital Collection System) olarak değiştirilmiştir. ABD kamuoyu tarafından yapılan tüm baskılara rağmen, bu sistemin FBI tarafından kullanıldığı, ne reddedilmiş ne de onaylanmıştır. Bu sistem aynı zamanda bir ISP'nin altyapısına bağlanarak bu ISP vasıtasıyla internet vasıtasıyla yapılan tüm trafik takip edilebilmektedir. Yazılım ve donanım ağırlıklı olan bu sistemde yer alan özel filtre programlarına aktarılan kelime ve kelime grupları taranarak bu ifadeleri içeren tüm e-posta trafiği ve haberleşmeleri, kimin kiminle, ne zaman ve mesajın içeriği de dahil olmak üzere gerekli tüm bilgiler gerçek zamanlı olarak FBI'nin sistemine yönlendirilmektedir.

Ancak her şeye rağmen Carnivore sisteminin kullanılmasının, 2001 yılında FBI tarafından terk edildiği 2005 yılında ilan edilmiştir. Bunun yerine daha da geliştirilmiş olan ve kod adı "DragonWare Suite" olan ve üç ayrı amaca yönelik olarak hazırlanmış olan "Carnivore", "Packeteer" ve "CoolMiner"dan oluşan bir sistem hizmete alınmıştır.

FBI bu ve buna benzer sistemleri daha ziyade suçluları, casusları, kaçakçıları ve teröristleri takip etmek amacıyla yoğun bir şekilde kullanmıştır. Söz konusu sistemin toplam maliyetinin 6-15 milyon ABD Doları olduğu ifade edilmektedir [5].

C. Echelon

Echelon sistemi küresel bir haberleşme müdahale (COMINT - Communications Interception) sistemi olup, tüm dünyadaki askeri ve sivil her türlü haberleşme izlenmekte ve kaydedilmektedir. Sistemin yönetimi, tamamen ABD'nin Ulusal Güvenlik Kurumu (NSA -

National Security Agency) olup, sistemin varlığı 1999 yılına kadar sürekli olarak inkar ediliyordu.

Ancak 16 Mart 1999'da Avustralya'daki Ulusal Askeri Muhabere Merkezi (DSD - Defense Signals Directorate) Müdürü Martin Bradley'in bir muhabir olan Ross Coulthart'a yazdığı mektupta ortaya çıktı. Bunun üzerine Avustralya hükümeti, Mayıs 1999'da yapılan bir açıklama ile Echelon sisteminin bir parçası olduklarını kabul etti.

Echelon sistemi esasen 2. Dünya Savaşı'ndan sonra ABD ve İngiltere arasında "UKUSA" adındaki bir anlaşmanın 1947'de imzalanması ile ortaya çıkmıştır. Daha sonra bu anlaşmaya Kanada, Avustralya ve Yeni Zelanda da taraf olmuştur.

Başlangıçta 1950'li yılların teknolojik kısıtlamaları nedeniyle sadece uluslararası teleks ve telefon trafiği izleniyordu. Ancak gelişen teknoloji sayesinde mikrodalga ve uydu teknolojileri dahil olmak üzere OCR, e-posta ve internet gibi bir çok farklı teknolojiler de izleme ve kaydetme sistemine dahil edilmiştir.

Sistem çok güçlü bir yazılım ve donanım altyapısına sahipti. Zira 1992 yılında NSA'den emekli olan ve buranın müdürlüğünü yapmış olan Amiral William Studeman'ın yaptığı açıklamaya göre Echelon sistemi, saatte 2 milyondan fazla telefon, teleks, e-posta ve faks mesajını izleyebiliyor ve kaydedebiliyordu ki bu rakam bir yılda 17,5 milyar mesaja karşılık gelmektedir. 1992 yılındaki teknolojik imkanlar sayesinde 2 milyon olan bu rakamın, günümüzde çok daha fazla bir değere ulaştığı düşünülebilir.

ECHELON dünyadaki iletişim trafiğinin çoğunu eş zamanlı olarak izleyebilmektedir. (elektronik posta, telefon, fax, telex, telgraf, kablo vs) İletişim eş zamanlı kompleks sözcük filtreleriyle izlenmektedir. Her dilde geliştirilen bu filtreler sayesinde anahtar sözcüklerin yakalandığı iletişimler değerlendirilmektedir.

ECHELON dünyada tek gözetleyici sistem değildir. Rusya (SORM), Fransa (Franchelon) ve Çin de benzeri sistemlere sahiptir. ECHELON sisteminin yaptığını e-posta trafiği üzerinde gerçekleştiren sistemler de bulunmaktadır. Diğer taraftan FBI'nın ilk kuşak internet gözetleme programının Etherpeek olduğu sanılmaktadır. Ayrıca Omnivore adındaki ikinci kuşak program ISP'nin bilgisayarlarına kurularak ISP'nin sunucusundan geçen e-postaları denetlemeye yarayan bir yazılım olarak 1997'de kullanılmaya başlanmıştır.

Echelon sayesinde yapılan tüm izleme ve kayıtlar doğrudan NSA ve CIA'ya yönlendirilmektedir. 11 Temmuz 2001 tarihinde Echelon sisteminin mevcut olup olmadığı konusunda AB Parlamentosu tarafından çok kapsamlı bir şekilde hazırlanan ve yayınlanan rapor, Echelon sisteminin mevcut olduğunu kanıtlamıştır. Ayrıca sözkonusu raporda Echelon sistemine benzer başka sistemlerin Rusya, Çin ve Fransa gibi bazı ülkelerde de kurulu olabileceği ifade edilmektedir [6].

VII. TEMPEST (TRANSIENT ELEKTROMAGNETIC PULSE SURVEILLANCE STANDARD)

Günümüzde sadece bilişimde değil, tüm bilgi ve iletişim teknolojilerinin her alanında güvenlik boyutu son derece önemlidir. Zira; virüs saldırıları ile TEMPEST örneğinde olduğu gibi, bilgisayarlara ve içindeki bilgilere çeşitli vasıtalarla yetkisiz ulaşım gibi sınır ötesi yapılan saldırı ve tehditlerin hepsi günümüz teknolojisinin beraberinde getirdiği en büyük risklerdendir. Bu nedenle, şebeke güvenliğinde sistemin daimi çalışabilirliği, doğrulama, verilerin bütünlüğü ve gizliliği olmak üzere dört temel unsur bulunmaktadır.

Bakır kablo ve monitör gibi ilave bazı donanımlardan oluşan tüm bilgisayar sistemleri, Van Eck adlı Hollanda'lı bilim adamının adına hitaben Van Eck denilen alıcılar tarafından alınabilen ve kaydedilebilen elektromanyetik yayınları yaymaktadır. Tempest teknolojisi, bu yayınların kullanılarak ve ortamdaki parazitlerden arındırılarak ve güçlendirilerek ilgili cihaz tarafından yaklaşık 500 m kadar uzaktan alınmasını engellemeye yönelik olarak oluşturulmuş bir teknolojidir.

Pasif bir saldırı teknolojisi olan Tempest'in esaslı şu hususa dayanmaktadır. Bilgisayarınızın klavyesinden, ekranından, modem kablosundan ve daha nice yerinden yayılan elektromanyetik salınımlar klavyede bastığınız tuşlara, ekranınızdaki görüntüye ve modeminizle bilgisayarınız arasında geçen bilgilere bağıntılıdır. Yeterli donanıma sahip herhangi biri bu yayınları bir veya iki kilometreye varabilen bir mesafeden kaydedebilir ve ekranınızda ne gördüğünü, klavyenizde ne girdiğinizi veya modeminizden ne geçtiğini bu yayınları işleyerek tekrar oluşturabilir [7].

A. Elektromanyetik Dinlemeden Nasıl Korunulur ?

Elektromanyetik güvenlik, bir bilgisayarın, veya herhangi bir elektrik/elektronik aygıtın çalışması esnasında yaydığı elektromanyetik ışınımların üçüncü bir kişi tarafından alınmasını ve/veya elde edilen işaretlerin işlenerek sözkonusu elektrik/elektronik aygıtın işlediği bilgilere ulaşılmasını engellemektir. Tempest kapsamında ekranlama, filtreleme veya yayılan dalgalara gürültü ekleyerek anlaşılabilir kılma gibi uygulanabilecek bazı elektromanyetik güvenlik yöntemleri mevcuttur.

Bu tip yöntemlerde ya doğrudan kullanılan elektronik malzemeler ekranlanır ve giriş/çıkışları filtrelenir veya ekranlı olması gerekmeyen aletler ekranlı odalarda (Faraday kafesi) kullanılır. Askeri ve diplomatik uygulamalarda genellikle ikinci yöntem kullanılır. Ekranlanacak odalar tamamen iletken bir maddeyle kaplanarak elektromanyetik yayınları durdurucu Faraday kafesi oluşturulur. Odaların havalandırma girişlerine dalga kırıcı yansıtıcılar konur. Elektrik şebekesine olan bağlantılar açıkverici işaretlerin bulunabileceği frekansları kesen filtreler

aracılığıyla yapılır. Bu tip odalar genellikle ses yalıtımına da tabi tutulur.

B. PGP (Pretty Good Privacy)

1991 yılında Philip Zimmermann tarafından gerçek bir güvenlik ve kişisel haklara saygı istediğinden dolayı gerçekleştirilen çalışmalar sonucu meydana getirilen ve PGP olarak adlandırılan bilgisayar programı, şifreleme vasıtasıyla gizliliği ve kimlik doğrulamayı sağlar.

Açık anahtar algoritmaları (asimetrik), simetrik şifreleme algoritmalarına göre nispeten yavaş olduğundan özellikle büyük dosyaların bu yöntemle şifrlenmesi durumunda işlem için oldukça uzun bir süre gerekmektedir. Bu nedenle şifrelemede kullanılan karışık algoritmalarda her iki yöntemin (simetrik ve asimetrik) artı yönlerinden yararlanılmaktadır. Yani orijinal veri, simetrik anahtar kullanılarak şifrelenir, daha sonra da simetrik anahtarın kendisi alıcının açık anahtarı kullanılarak şifrelenir ve mesajın sonuna eklenir. Şifre çözme işlemi sırasında, alıcının gizli anahtarı kullanılarak öncelikle simetrik anahtar elde edilir, ardından simetrik anahtarla mesajın kendisi çözülür. Bu yöntemi kullanan tekniklerden biri de PGP'dir. Standardı RFC 2440 olan PGP'de işin simetrik kısmı için IDEA, asimetrik kısmı için ise RSA algoritması kullanılmaktadır.

Özetle PGP, açık anahtarlı kriptografinin sahip olduğu avantajlardan faydalanarak kişilerin birbirlerine elektronik ortamda gönderdikleri mesajların bütünlüğünü, gizliliğini, mesajın kim tarafından gönderildiğini teyit eden bir uygulamadır.

Açık anahtarlı kriptografi de, birisi şifreleme ve diğeri de şifreyi çömek için iki adet anahtar çifti kullanılır. Matematikte kullanılan asal sayıların çarpınlarına ayrılması ilkesinden hareketle bu anahtar çifti, matematiksel açıdan birbirleri ile ilişkili olmakla beraber, birisinden yararlanarak diğersinin bulunması son derece zordur.

Sayısal imza kullanımı için kullanımı oldukça kolay ve güvenli bir program olan PGP, ayrıca şifreleme, şebeke güvenlik uygulamaları ve güvenlik duvarı gibi başka uygulama alanlarında da kullanılmaktadır. Ayrıca PGP'de mesaj şifrlenmeden önce sıkıştırılır ki, bu da transfer edilecek bilgi miktarından daha fazla tasarruf edilmesini sağlar ve mesajın deşifre edilmesi olasılığını da azaltır.

PGP ile dosya, mail ve mesajların güvenliği sağlanabileceği gibi bir bilgisayar ile diğer bilgisayar ve bilgisayarlar arasında güvenli oturumlar açılabilir. Bu sayede bilgisayarlar arasındaki iletişim büyük ölçüde güvenlik altına alınmış olur. PGPNet kullanılması halinde örneğin internet explorer veya e-posta programlarında şifrelemeye veya sayısal imza kullanımına gerek kalmaz. Böyle bir durumda işlemler normalde yapıldığı gibi yapılabilir ve iletişim güvenlidir. Bunun için PGP ile gelen PGPnet

programının VPN ve VI (Virtual Identity) özellikleri kullanılır.

Güvenli e-posta, dosya şifreleme protokolü olan PGP'de IDEA, RSA, DSA, MD5 ve SHA-1 gibi bir dizi şifreleme algoritması desteklenmektedir. PGP sayesinde e-posta ve dosyalar, istenmeyen kişiler tarafından ele geçirilse dahi, eğer PGP ile şifrelenmişse bu dosyaların içeriklerine ulaşılamaz.

PGP'nin algoritması kamuya açık olup oldukça güvenlidir. Zira algoritması açık olmayan bir şifre standardına güvenilemez. Örneğin ABD hükümeti kendi şifreleme standartlarını ortaya çıkarmaktadır, ancak bunlar hükümet odaklı şifreleme standartları olduklarından, genelde kodları yayınlanmaz. Bu nedenledir ki PGP özellikle teröristler ve diktatörlük ile yönetilen ülkelerde güvenli e-posta haberleşmesinde çok sık kullanılmaktadır. Çünkü e-postada taşınan önemli ve/veya kişisel bilgilerin, güvensiz bir şekilde internette dolaştığından dolayı e-posta güvenliğine bu kadar önem verilmektedir. Ancak PGP'de e-posta başlıkları şifrelenmediğinden, e-posta başlıklarında "Top Secret" gibi dikkati çekecek ifadeler kullanılmamalıdır [8].

VIII. SONUÇ VE DEĞERLENDİRMELER

Günümüzün en değerli ve korunması gereken varlığı haline gelen bilgiyi korumada önemli ilerlemeler kaydetmiş ülkeler gelişmişlik düzeyinde önemli iyileşmeler sağlamıştır.

Türkiye'nin de gelişmiş ülkeler seviyesine ulaşması, ekonomik değişim ve toplumsal dönüşümünü tamamlayabilmesi ve rekabetçi dünyada yerini alabilmesi için, bilgi ve iletişim teknolojileri üzerinde saklanan ve aktarılan bilginin güvenliğini ve kişisel mahremiyetini sağlaması gereklidir.

Güvenlik açısından göz önüne alınması gereken husus, güvenlik alanlarının çok iyi tespit edilerek bilginin özelliğine en uygun önlemlerin alınmasıdır. Ancak ünlü hacker Kevin Mitnick'in "Kırılmayacak site, sızılmayacak ağ yoktur" sözünden de anlaşılacağı üzere tam olarak bilgi güvenliğinden söz etmek mümkün olamamaktadır. Ancak, bu konuda atılacak en önemli adım etkin ve verimli bir güvenlik kültürünün oluşturulması, bilgi güvenliğinin temel unsuru olan kişisel verilerin korunması ile ilgili düzenlemelerin yapılması ve küresel bir ağ haline gelen bilgi ve iletişim teknolojilerinde uluslararası işbirliğine önem verilmesinin şart olduğu değerlendirilmektedir.

Hükümetin, tüm kesimden kullanıcının katılımını sağlayacak bir "Eylem Planı"na başlatması, bilgi sistemlerinin güvenliği için ulusal politika geliştirmesi ve diğer ülkeler ile işbirliği yapması, eğitimler, broşürler, internet siteleri hazırlaması ve danışma birimleri kurması, konu ile ilgili uluslararası standartları Türk Standardı haline getirmesi ve kullanımını

sağlaması, tüm kurumların, özel kuruluşların ve sivil toplum kuruluşlarının işbirliği içinde bulunmasını sağlaması, bilgi güvenliğini sağlayacak yasal düzenlemelerin bir an önce yürürlüğe girmesini sağlaması, bilgi teknolojilerinin gelişimi için araştırma-geliştirmenin devletçe desteklenmesi, bilgi güvenliği ve kişisel mahremiyete yönelik ihlalleri asgari düzeye indirecek cezai önlemlerin alınmasını sağlaması, bilişim suçları ile ilgili birimler kurması, diğer ülkelerde olduğu gibi bilgi güvenliği konusunda kişileri yönlendirebilecek ve olaylara müdahale edebilecek CERT gibi kurumlar kurması, gereklidir. Ayrıca bu konuda uluslararası işbirliğinin önemli olması nedeniyle diğer ülkelerle işbirliği kurma yoluna gitmesi gerekmektedir.

Kurum ve kuruluşların, kendi yapılarına uygun “Kurumsal Güvenlik Politikası” geliştirmesi, bilgi güvenliği konusunda oluşturulan standartların kullanımına özen göstermesi gerekmektedir.

Kullanıcıların, bilgi sistem ve ağlarındaki diğer kullanıcılara karşı sorumlu olduklarının bilincinde olması, güncel antivirüs yazılımı ve lisanslı yazılımlar kullanması, İnternette kişisel verilerini nasıl koruyacaklarını bilmesi, bilgisayar ve e-postaları için parola kullanması ve bunları sık sık güncellemesi, güvenmedikleri sitelere girmemesi ve tanımadıkları kişilerden gelen e-postaları açmaması gerekmektedir.

Güvenlik kültürü oluşturulmasında her kurum, kuruluş ve bireye sorumluluk düşmesi nedeniyle Telekomünikasyon Kurumu’nun da “Kurumsal Bilgi Güvenliği Politikası” oluşturması, Kurum çalışanlarının elektronik ortamda tutulan ve aktarılan bilginin güvenliğini sağlama hususunda uyması gereken kural ve politikaları belirlemesi gereklidir.

İSS’lere bilgi güvenliği ihlallerini önleme yetkisi ve yükümlülüğü verilmelidir. İSS’lerin aboneleri ile yaptıkları sözleşmede kendi abonelerinin bilgi güvenliği ihlali yapamayacakları hüküm altına alınmalı ve kendi abonesinin ihlalden İSS sorumlu tutulabilmelidir. Ayrıca abonelerinin hazırlamış oldukları İnternet sitelerinde özellikle ticari sitelerde gizlilik politikalarının ne olduğu kişisel bilgilerin niçin istendiği, bilgilerin hangi amaçla kullanılacağı ve bilgilerin güvenliğinin nasıl sağlanacağına ilişkin bilgilerin sunulması sağlanmalıdır. Bununla birlikte siteler, “çerez” (cookie) gönderilip gönderilmediği konusunda kullanıcıyı bilgilendirmeli ve kullanıcıya bunu reddetme imkanı tanınmalıdır.

Kurumun “Kişisel Verilerin Korunması Kanunu”nun yasallaşmasının ardından kurulacak olan “Kişisel Verileri Koruma Kurumu” ile yakın ilişkide ve istişarelerde bulunarak telekomünikasyon alanında kişisel verilerin korunması hususunda ortak politikalar gerçekleştirmesi gereklidir. Bu gerçekleştirilen politikalar ışığında işletmecilere, abone ve kullanıcılara dair kişisel verilerin korunması konusunda yükümlülükler getirilmelidir.

Kurum önderliğinde tüm sektör aktörlerinin katılımı ile oluşturulacak ve “Elektronik Haberleşme Sektöründe Kişisel Verilerin ve Mahremiyetinin Korunması Komisyonu” olarak adlandırılacak bir komisyon sayesinde abone ve kullanıcılar dahil olmak üzere tüm sektör aktörlerinin yapacağı toplantılarda karşılıklı bilgi alış veriş ve istişarelerde bulunarak kişisel verilerin ve mahremiyetin korunmasına yönelik olarak ilgili mevzuatın varsa eksikliklerinin tespiti, usul ve esasların belirlenmesi, mevzuatın nasıl daha iyi ve sağlıklı olarak işletilebileceğinin değerlendirilmesi gereklidir.

Kurumun diğer ülkelerdeki düzenleyici kurumlarla ikili işbirliği geliştirerek, onların telekomünikasyon alanında kişisel verilerin ve mahremiyetin korunması konusunda yaptıkları tecrübelerden faydalanması, edindiği izlenim ve tecrübeleri sektöre aktarması oldukça büyük önem arz etmektedir.

Kurumun, AB mevzuatını uyumlaştırma sürecinde, istek dışı haberleşme konusuna önem vererek bu konuda bir an önce yasal düzenleme çalışmalarına başlaması, bu konuda sorumluluk ve yaptırımları belirlemesi gereklidir. Yapılacak yasal düzenleme ile, abonenin önceden rızası olmadan istek dışı haberleşme yapılmasının önlenmesi, gerçek ve tüzel kişilerin kendi müşterilerine çıkan yeni bir ürün veya hizmet hakkında bilgi vermek amacıyla mesaj gönderebilmesi, ancak mesajın içeriğinde mesajı gönderenin açık bir şekilde belirtilmesi ve alıcının mesajı tekrar almak istememesi durumunda ücretsiz ve kolay bir yolla reddedilme imkanının tanınması, mesajın içeriğinin ahlaka ve kamu düzenine aykırı olmaması, mesaj gönderen kişilerin sahte isim ve şaşırtıcı konu başlığı kullanmalarının önlenmesi, kişinin rızası olmamasına rağmen mesajın zorla gönderilmemesi, ahlaka ve kamu düzenine aykırı olması durumunda cezai müeyyidelerin konulması, pornografik içerikli mesajların gönderilmesinin yasaklanması sağlanmalıdır. Bunun yanı sıra, diğer AB üyesi ülkelerde olduğu gibi kapsam içi yöntemin uygulanması gereklidir.

Kurum bünyesinde veya İSS’ler bünyesinde oluşturulacak kapsam içi veya kapsam dışı yöntem ile elektronik posta yoluyla istek dışı ticari reklam yapacak kişilerin kayıtları tutularak bu tarz reklamları almak istemeyen gerçek kişilerin buraya başvurarak kapsam içi veya kapsam dışı kaydı yaptırımları sağlanmalı ve kayıtlar sık sık güncellenmelidir. Bu listelerin Kurum internet sayfasında yayınlanması istek dışı haberleşmeyi önleme konusunda yardımcı olacaktır. Bunun yanı sıra istek dışı haberleşme alan kişilerin bunu iletebilecekleri birimler kurulmalıdır.

Bilgi toplumunun oluşturulması ve yaygınlaştırılmasında en büyük engel olarak görülen istek dışı haberleşmenin artması toplumun hemen hemen tüm kesiminin (internet kullanıcıları, kamu sektörü, İSS’ler, hizmet sağlayıcılar) ortak kararlılığı, yapılacak işbirliği ve dayanışmayla oluşturulacak mücadelede başarı sağlayabilecektir. Bu itibarla Kurum diğer ilgili kurum ve kuruluşların işbirliği ile istek dışı

haberleşmeyi önleme konusunda görüş, öneri ve politikaların oluşturulacağı forumlar düzenlemelidir.

Ayrıca, İSS'lere istek dışı mesajları bloke etme yetkisi ve yükümlülüğü verilmelidir. Diğer taraftan İSS'lerin aboneleri ile yaptıkları sözleşmede kendi abonelerinin istek dışı haberleşme gönderemeyecekleri hüküm altına alınmalı ve kendi abonesinin gönderdiği istek dışı mesajdan İSS sorumlu tutulabilmelidir.

İstek dışı haberleşmenin önlenmesinde uluslararası işbirliğinin önemli olması nedeniyle Kurumun istek dışı haberleşme konusunda uluslararası işbirliğine önem vermesi, diğer ülkelerin konuyla ilgili kuruluşları ile istişarelerde bulunması ve istek dışı haberleşmeyi önleme konusunda ikili işbirliği anlaşmalarını hayata geçirmesi gereklidir.

Sadece bilgi ve iletişim teknolojileri boyutunda değil, günümüz kullanıcılarında olduğu kadar üretici ve işletmeciler gibi daha bir çok sektör aktörlerinin hepsinde ortak duyulan bir endişe sözkonusudur. **“Güvenlik”**. Zaten konu ile ilgili olarak çeşitli platformlarda halen çalışmaları yürütülmekte olan tüm standardizasyon faaliyetlerinin temel hedefi sistem ve cihazlar arasında uyumlu çalışabilmeyi sağlamak olduğu kadar, güvenlik unsuru da birinci derecede rol oynamaktadır. Bilgi güvenliği kavramı içinde kişisel ve kurumsal güvenlik gibi temel hususlar yer almakla birlikte, bunların altında iletişim ağı güvenliği, işletim sistemi güvenliği, veri tabanı güvenliği, internet erişim güvenliği, terminal cihazı ve sistem güvenliği gibi oldukça önemli hususlar bulunmaktadır. Özetle, burada sayılanların hepsinin **“Toplam Sistem Güvenliği”** adı altında toplanması mümkündür.

Yukarıda da belirtildiği üzere, bilgi ve iletişim teknolojileri alanında AB, özellikle ABD ile arasındaki büyük farkı kapatabilmek için hazırlanmış olduğu 2002 ve 2005 Eylem Planları çerçevesinde AB halkının bilgi toplumu haline gelerek geniş bantlı teknolojilerden büyük ölçüde yararlanabilmesini hedeflenmiştir. Örneğin, İsveç GSYİH'sının 10,5'ini bilgi ve iletişim teknolojilerine ayırırken İspanya %5'ini ayırmaktadır. Diğer AB üyesi 12 ülkedeki oranlar bu iki rakam arasında seyretmektedir.

Bu rakamlar, geniş bantlı teknolojilerin toplum bazına yaygınlaştıkça veri güvenliği olgusunun beraberinde getireceği muhtemel risklerin ve siber saldırıların da doğru orantılı olarak artacağına işaret etmektedir. Dolayısı ile, konu sadece bilgisayar suçlarına yönelik olarak ülkelerde görevli bir Kuruma işlerlik kazandırılmasını değil aynı zamanda yargı organları, sanayi, tüketici kuruluşları, üniversiteler ve veri koruma kurumları arasında işbirliğinin artırılmasını ve geliştirilmesini gerektirmektedir. Bununla beraber, bilgi ve iletişim teknolojilerinde veri güvenliğinin belki de en önemli kısmını oluşturan telekomünikasyon işletmecileri ile erişim sağlayıcılarının gelişen teknoloji çerçevesinde tesbit edilecek olan asgari seviyedeki güvenlik kriterlerine uymaları da büyük önem arz etmektedir. Bu bağlamda **“siber-suç polisi”** ve

“siber-suç savcısı” gibi yeni tanım ve meslek dallarının ya da diğer bir deyişle bilgi ve iletişim teknolojileri alanında veri güvenliği konusunda hukuki ve teknik ihtisas gerektiren yeni branşların gündeme gelmesi bir teknolojik zorunluluk olarak ortaya çıkmaktadır.

Bu çerçevede; bilgi ve iletişim teknolojileri alanında bilgi güvenliği ve mahremiyetin korunmasına yönelik olarak AB'de halen çok çeşitli platformlarda mevcut çalışmalar, dikkate alınır ise, konu sadece Ülkemizin AB'ne uyumu açısından değil; aynı zamanda günümüz teknolojisinin gereklerine ve ihtiyaçlarına mümkün olan en kısa sürede uyum sağlayabilme ve hatta gerçekleştirilebilir ise; Ülkemizde başta bilgi ve iletişim teknolojilerinde veri güvenliği olmak üzere, diğer teknolojik alanlarda da **Devlet-Sanayi-Üniversite** işbirliğinin geliştirilebilmesi için, sözkonusu çalışmaların mümkün olan en kısa sürede başlatılmasının, Ülkemiz menfaatleri açısından doğru bir yaklaşım olacağı değerlendirilmektedir. Zira burada önemli olan husus, bir çok gelişmiş ülkede yazılım ve donanım ürünleri dahil olmak üzere bilişim sektörünün **“Stratejik Sektör”** olarak ilan edildiği olgusunun gerektirdiği ölçüde Ülkemizde topyekün bir işbirliğinin ve eyleminin gerektiridir.

Bu çerçevede ülkemizde başta Telekomünikasyon Kurumu olmak üzere, Ulaştırma Bakanlığı gibi ilgili tüm kamu kurum ve kuruluşlarının ve diğer sektör aktörlerinin de iştirakinin sağlandığı **“Bilgi Güvenliği Ulusal Koordinasyon Kurulu”**nun kurulması son derece önem arz etmektedir. Kurulun temel amacı, telekomünikasyon sektöründeki abone ve kullanıcılar dahil olmak üzere tüm sektör aktörlerinin ve ilgili kamu kurum ve kuruluşlarının iştirak edeceği toplantıların düzenlenmesi ve bu çerçevede ilgili tüm taraflar arasında bilgi, tecrübe ve doküman paylaşımının yapılmasıdır. Ayrıca **“Bilgi Güvenliği Ulusal Koordinasyon Kurulu”** tarafından yürütülecek çalışmaların kapsamı ise, ilgili taraflarla karşılıklı bilgi alış veriş ve istişarelerde bulunarak bilgi güvenliğinin teminine yönelik olarak ülkemizde ihtiyaç analizinin yapılması, hazırlanacak rapor ışığında alınabilecek hukuki ve teknik tedbirlerin tespit edilmesi ve bu kapsamda yapılabilecek önerilerin değerlendirilerek ülkemiz açısından bir raporun hazırlanması olarak belirlenmelidir.

KAYNAKLAR

- [1] European Innovation, May 2007, pp. 8
- [2] http://ec.europa.eu/information_Society/index_en.htm
- [3] L. Morley, Identity Crisis, pp. 7. Available: www.eurocomms.co.uk
- [4] http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml
- [5] www.foxnews.com
- [6] <http://en.wikipedia.org/wiki/echelon>
- [7] S. Capkun, System Security, pp. 6
- [8] www.wsws.org