Siber Savunma: Ülkeler ve Stratejiler

Mehmet MERAL

***Özet*-1980'lerde bilgisayarların birbirleriyle iletişim kurmasıyla başlayan siber mekan kavramı muazzam bir gelişme kaydetmiştir. İnternet yakın zamana kadar bireyler ve iş çevreleri tarafından önem verilen ancak ulusal güvenlik veçhesi olmayan bir olgu olmakla birlikte, son zamanlarda milyarlarca internet kullanıcısı tarafından oluşturulan bu siber mekan güvenlik açısından etkin bir şekilde kontrol edilememektedir. Bu nedenle siber-savunma, siber-güvenlik, siber-saldırılar gibi kavramlar ulusal güvenlik bakımından önem arzetmeye başlamıştır. Bu çalışmada önde gelen ülkelerin siber savunma alanında yaptığı çalışmalar ve siber saldırılara karşı uyguladıkları stratejiler tanıtılmıştır.**

***Anahtar kelimeler*- Siber savunma, siber güvenlik, siber saldırı, strateji**

I. GİRİŞ

Siber bilişim yapılarının bankacılık, ulaşım, iletişim gibi temel alanlardaki ağırlığı, bu yapıların ve bu yapılarda saklanan bilgilerin güvenlik boyutunu konunun ayrılmaz bir parçası hailne getirmiştir. Küreselleşme ve bilgi teknolojilerinin yayılmasıyla birlikte özellikle düşük maliyetli olması, çok sayıda insan üzerine etki edebilmesi gibi nedenlerle siber saldırıların aynı zamanda teröristlerce artan bir şekilde tercih edildiği görülmektedir. Uzmanlar siber-güvenlik konusunda "uluslararası işbirliği, ulusal bilinçlenme ve bireysel bilinçlenmenin" elzem olduğunu ifade etmektedirler. NATO gibi uluslararası kuruluşlar siber-güvenliğe ilişkin ulusal sorumluluklara büyük önem vermektedir. Bu büyük tehiditlerin farkında olan gelişmiş ülkeler ise ulusal anlamda yaptıkları örgütlenmelerle siber savunmaya yönelik yasal düzelemeler, strateji belgeleri ve eylem planları hazırlayarak olası bir siber saldırı, siber savaş durumuna karşı hazırlıklı olmak için ulusal önlemler ve uluslararası işbirliği temelinde önemli adımlar atmışlardır.

Bu çalışmanın ikinci bölümünde konuyla ilgili tanımlar verilmiş, üçüncü bölümünde gelimiş ülkelerde siber savunma bağlanımda yaplan çalışmalar tanıtılmış, dördüncü bölümünde ise genel bir değerledirme sunulmuştur.

MEHMET MERAL, Dışişleri Bakanlığı 06100 Balgat Ankara (e-mail: mehmet.meral@mfa.gov.tr)

II. TANIMLAR: SİBER MEKAN, SİBER TERÖRİZM, SİBER SAVUNMA

Siber mekan: Network sistemleri ve ilgili fiziksel alt yapıyla bilgi depolamak, değiştirmek için kullanılan elektronik ve elektromağnetik ortamdır.

Siber terörizm: Bilgisayarlara ve içlerinde depolanan bilgilere karşı siyasi, sosyal veya ekonomik amaçlarla girişilen kanunsuz saldırılar veya saldırı tehditlerdir.

Siber savunma: Siber mekanı siber saldırılara ve siber terörizme karşı korumak için uygulanan güvenilk yöntemleridir.

III. DÜNYA ÜLKELERİ VE SİBER SAVUNMA STRATEJİLERİ

A. NATO

NATO, 21. yüzyılda dönüşüm sürecinde güvenliğe ilişkin hususlara büyük önem vermektedir. Enerji güvenliği ve siber güvenlik gibi yeni küresel tehditlere karşı NATO üyeler bağlamında savunma stratejileri geliştirmektedir. 2005 yılında Estonya ve Rusya arasında yaşanan gerginlikten sonra ise NATO Estonya'da Siber Savunma Mükemmelliyet Merkezi kurmuş, faaliyetlerini bu organizasyon çerçevesinde yürütmektedir. 2007 yılında hazırlanmaya başlayan Siber Savunma Siyasası ise taslak halinde olup henüz üzerinde mutabakat sağlanmamıştır.

B. ABD

ABD'nin siber savunma alanındaki faaliyetlerine ilişkin temel belgeyi Şubat 2003 tarihli "The National Strategy to Secure Cyberspace" oluşturmaktadır. Federal Yönetim, yerel makamlar ile özel sektörü içermesi nedeniyle ulusal nitelikte ve geniş kapsamlı olan anılan belgede, kendi görev alanları itibarıyla öncü rol üstlenecek devlet kurumları da belirtilmektedir. Bu çerçevede, örneğin bankacılık sektörü için Hazine Bakanlığı, elektrik ve gaz şebekeleri için de Enerji Bakanlığı esas makam olarak gösterilmektedir. Bahsekonu strateji belgesinin, "National Strategy for Homeland Security" belgesinin uygulama boyutunu oluşturduğu ve "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" belgesini tamamlayıcı nitelikte olduğu belirtilmektedir.

Gerek anılan belge gerek 17 Aralık 2003 tarihli İç Güvenliğe ilişkin Başkanlık Direktifi uyarınca, İç Güvenlik Bakanlığına (Department of Homeland Security) siber savunma konusuda önemli sorumluluklar verildiği anlaşılmaktadır.

C. ALMANYA

Almanya'nın elektronik ortamda gerçekleştirilebilecek saldırılara karşı almakta olduğu önlemler Federal İçişleri Bakanlığı tarafından hazırlanan "Enformasyon Altyapı Savunması İçin Ulusal Plan" başlıklı belgede tanımlanmıştır. Alman makamları, elektronik saldırıların başlıca hedefini büyük şirketler, bankalar veya kamu kuruluşları olarak tanımlamışlardır. Ulusal Plan'ın uygulanmasının koordinasyonu, "Enformasyon Güvenliğinden Sorumlu Federal Ofis" (BSI) tarafından yürütülmektedir. Bu saldırılara karşı koyabilmek için Federal Hükümet, Ulusal Plan'da üç stratejik hedef belirlemiştir:

1. Önleme: Bu başlık altında, enformasyon altyapısının, güncel ve güvenli teknoloji ürünlerinin kullanımı ve mevcut risklerlerin bilinciyle uygun şekilde korunması öngörülmektedir.
2. Hazırlıklı olma: Meydana gelebilecek elektronik saldırılara etkin şekilde karşı koyabilmek için BSI bünyesinde Enformasyon Teknolojisi Kriz Müdahale Merkezi tesis edilmesi planlanmakta, bu merkezin ulusal komuta, kontrol ve analiz merkezi görevlerini üstlenmesi ve bu amaçla bir algılayıcı ağı kurulması hedeflenmektedir. Aynı şekilde, Federal Hükümet, halkın ve özel sektörün mevcut riskler ve alınabilecek önlemler hakkında bilinçlendirilmesini hedeflemektedir.
3. Sürdürülebilirlik: Bu başlık altında, Almanya'nın elektronik güvenlik alanında yeterliliğinin artırılması amaçlanmaktadır.

Sözkonusu belgenin uygulanmasında gerekli önlemlerin Federal Hükümet tarafından alınması öngörülmektedir. Bununla beraber, uygulamaların sadece yetkili makamlar tarafından yerine getirilmesinin yeterli olmayacağı gerçeğiyle özel kuruluşlarla işbirliği hedeflenmektedir. Bahsekonu belgede, özel kullanıcıların da mevcut risklerin bilincinde olmalarının ve gerekli bireysel önlemlerin alınmasının önemine dikkat çekilmekte, öte yandan ülkelerarası işbirliğine de vurgu yapılarak, Almanya'nın uluslararası standartların ve normların tesis edilmesini savunduğu kaydedilmektedir.

D. DANİMARKA

Danimarka'da sanal alemden gerçekleştirilen saldırılara karşı koymakla görevli tek bir otorite bulunmamakta, görev ve yetki;

- Danimarka İstihbarat ve Güvenlik Servisi (PET),
- Savunma Bakanlığı'na bağlı Danimarka Kriz Yönetim Makamı (DEMA),
- Bilim, Teknoloji ve Yenilik Bakanlığı'na bağlı Danimarka Ulusal Bilgi Teknolojileri ve Telekomünikasyon Kurumu (ITST) ve
- Bağımsız idari otorite statüsünde bulunan ve teknoloji ile ilgili konularda, parlamento ile kamu kurumlarını bilgilendirmekle görevli Danimarka Teknoloji Kurulu arasında paylaştırılmış durumdadır.

Danimarka Teknoloji Kurulu himayesinde "IT- security Beyond Borders" adıyla kurulan bir çalışma grubunca 2007'de sınırı aşan bilgi teknolojileri güvenliği meselelerine dair bir rapor yayımlanmıştır. Raporda, bu alanda uluslararası yardımlaşmanın önemine ve somut adımlar atılması gerektiğine özel vurgu yapıldığı anlaşılmaktadır.

Danimarka İstihbarat Servisi konuya dair kamu kurum ve kuruluşlarına rehberlik ve yardım hizmetlerinde bulunmakta, yine korunmasında kamu yararı bulunan bilgileri haiz kişilere de gerekli yardımları yapmaktadır. Öte yandan, son yıllarda elektronik verilerin depolanması ve iletilmesindeki artışın sonucu olarak PET bünyesinde bilgi teknolojileri güvenliği kısımı (IT security section) tesis edilmiştir. Bu bağlamda PET ulusal ve uluslararası makamlarla (istihbarat makamları dahil) işbirliği halinde faaliyetler yürütmektedir.

E. FİNLANDİYA

Finlandiya'da elektronik ortamdaki saldırılara karşı savunma konusunda yetkili makam Fin İletişim Düzenleme Kurulu (Finnish Communications Regularity Authority)'dur. Elektronik ortamdaki saldırılarla mücadele dahil olmak üzere, bilgi güvenliğinin sağlanması için önlemler alınması ve bilgi güvenlik durumunun geliştirilmesinde yetkili ve sorumlu en üst makam Hükümet'tir. Hükümet, Eylül 2003'te Ulusal Bilgi Güvenliği Stratejisi hakkında kararı kabul etmiştir. Sözkonusu stratejinin desteklenmesi ve kaydedilen gelişmelerin gözetimi, Ulusal Bilgi Güvenliği Danışma Kurulu (National Information Security Advisory Board) tarafından 2007 yılı başlarına kadar yerine getirilmiştir. Anılan Kurul'un 2004 yılında Hükümet'e sunduğu "Creating a Safer Information Society" başlıklı raporunu sunmştur.

Bilgi güvenliğinin sağlanması için 2008 yılında Bakanlıklararası bir çalışma yapılarak yeni bir strateji belgesi hazırlanmaktadır. Bu çalışmayı "Ubiquitous Information Society Advisory Board" (Geniş Bilgi Toplumu Danışma Kurulu) altında kurulan yeni bir bilgi güvenliği grubu yerine getirmektedir.

Olağan durumlarda, bilgi güvenliğinin sağlanması ve bu konuda yapılacak düzenlemelere öncülük edilmesi, Ulaştırma ve İletişim Bakanlığı, sözkonusu Bakanlığa bağlı Fin İletişim Düzenleme Kurulu ve Ekonomi ve İstihdam Bakanlığı tarafından gerçekleştirilmektedir. Kamu sektöründe bilgi güvenliğinin geliştirilmesi ise, temel olarak Maliye Bakanlığı ile İçişleri Bakanlığı'nın sorumluluğundadır. Ulaştırma ve İletişim Bakanlığı, iletişim hizmetlerinde bilgi güvenliğiyle ilgili mevzuat ve strateji geliştirmeden sorumludur. Anılan Bakanlık, bu çerçevede, Fin halkına, iş dünyası ve kamu sektörüne bilgi toplumunda sunulan tüm hizmetlerin kullanılabilirliği ve güvenliğini, ayrıca özel bilgilerin korunmasını sağlamakla yükümlüdür.

CERT-FI, Fin İletişim Düzenleme Kurulu'nun bilgi güvenliği ihlalleri ve bu ihlallerin önlenmesi konularında yetkili birimidir.

F. FRANSA

Fransa'da elektronik ortamda gerçekleştirilebilecek suç ve saldırılarla mücadeleden sorumlu tek bir birim bulunmamakta; suçun niteliğine göre farklı birimlere sorumluluk verilmektedir. Bunlar arasında en önemlileri

- Başbakanlığa bağlı Milli Savunma Genel Sekreterliği
- İçişleri Bakanlığı'nın Adli Polis birimine bağlı olarak faaliyet gösteren "Bilişim Teknolojileri ile İlgili Suçlarla Mücadele Dairesi" - Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information de la Communication (OCLCTIC) dir.

Yukarıda kayıtlı iki kurumun dışında, Ekonomi, Maliye ve Çalışma Bakanlığı'na bağlı Telekom idaresi, Adalet Bakanlığı ve Jandarma Kuvvetlerinin de siber suçlarla mücadelede görevleri bulunmaktadır. Siber suçlar, Ceza Kanunu'nun (Code Pénal) 226. ve 323. maddeleri çerçevesinde cezalandırılmaktadır. Posta ve Elektronik Haberleşme Kanunu (Code des Postes et des Communications Electroniques) ise, siber haberleşme alanına bazı düzenlemeler getirmektedir.

G. GÜNEY KORE

İnternet kullanımının son derece yaygın olduğu Güney Kore'de elektronik ortamdaki saldırılara karşı savunma, farklı yönleriyle farklı kuruluşları ilgilendirmektedir. Toplantılarını Cumhurbaşkanı başkanlığında gerçekleştiren ve Cumhurbaşkanına iç ve dış politika ile askeri konuların ulusal güvenlik boyutu hakkında bilgi vermekten sorumlu olan "Ulusal Güvenlik Konseyi"nin sekreteryası, ulusal kriz uyarı sisteminin işleyişi ve geliştirilmesi, ulusal kriz durumlarına ilişkin bilgilerin toplanması, özetlenmesi ve dağıtılması ile siber tehdit uyarısı yayınlanmasından da sorumludur. "Ulusal Güvenlik Konseyi" bünyesinde yer alan "Ulusal Siber Güvenlik Strateji Konseyi" (National Cyber Security Strategic Council) ise ulusal siber güvenlik sisteminin kurulması ve geliştirilmesi, siber güvenlik politikaları ve çeşitli kuruluşlar arasında eşgüdümün sağlanması ve Cumhurbaşkanının siber güvenliğe yönelik kararlarının uygulanmasından sorumludur. Güney Kore Ulusal İstihbarat Servisinin başkanı aynı zamanda bu Konseyin de başkanıdır.

"Ulusal Siber Güvenlik Strateji Konseyi"nin altında, "Ulusal Siber Güvenlik Konseyi" (National Cyber Security Council) yer almaktadır. Siber güvenliğin sağlanması ve "Ulusal Siber Güvenlik Strateji Konseyi" tarafından alınan kararların uygulanması "Ulusal Siber Güvenlik Konseyi"nin görev alanına girmektedir. Konseyin başkanlığını, Güney Kore Ulusal İstihbarat Servisinin başkan yardımcısı yapmaktadır. Konsey, "Ulusal Güvenlik Konseyi Kriz Yönetim Merkezi" (NSC Crisis Management Center) Müdürü, "Ulusal Siber Güvenlik Merkezi" (National Cyber Security Center) Müdürü, Savunma Bakanlığı Enformasyon Dairesi Genel Müdürü ile Enformasyon ve Haberleşme Bakanlığı Enformasyon Planlama Yetkilisinden oluşmaktadır.

Elektronik ortamdaki saldırılara karşı savunma politikalarının hayata geçirilmesinden özel sektörü ilgilendiren konularda Enformasyon ve Haberleşme Bakanlığı bünyesindeki "Kore Enformasyon Güvenlik Ajansı"na (Korea Information Security Agency) bağlı "Kore Internet Güvenlik Merkezi" (Korea Internet Security Center); ülke savunmasını ilgilendiren konularda Savunma Bakanlığına bağlı "Enformasyon Savaş Müdahale Merkezi"(Information Warfare Response Center), ulusal güvenliği ve kamu sektörünü ilgilendiren konularda ise Ulusal İstihbarat Servisine bağlı "Ulusal Siber Güvenlik Merkezi" (National Cyber Security Center) sorumludur. Ayrıca, Güney Kore ulusal polis teşkilatı bünyesinde de "Siber Terör Müdahale Merkezi" (Cyber Terror Response Center) bulunmaktadır.

H. İNGİLTERE

İngiltere'deki uygulamada, elektronik ortamdaki saldırılara karşı savunma konusu "bilgi güvenliği" (information assurance) kapsamında ele alınmaktadır. Bilgi güvenliği konusundaki çalışmalar, teknolojik gelişmelere paralel olarak İngiltere'de 1999 yılından sonra ağırlık kazanmıştır. Kamu ve özel sektörün bu kapsamdaki ihtiyaçlarının karşılanması amacıyla üçlü bir yapı tesis edilmiştir.

Başbakanlık ofisine (cabinet office) bağlı olarak görev yapan "Central Sponsor for Information Assurance", "cyber defense" konusunda politika, strateji ve siyasa geliştirme çalışmalarını yürütmektedir. Hazırlanan sözkonusu politikaların uygulamasından ise "Center for Protection of National Infrastructure" (CPNI) ve "The Communications-Electronics Security Group" (CESG) sorumludur.

CPNI özel sektör ve iş çevrelerinin, CESG ise kamu kuruluşlarının bu alandaki ihtiyaçlarının karşılanmasında rol almakta, elektronik altyapı ve bilgi ağlarına yönelik olarak gerçekleştirilebilecek saldırılar konusunda ilgili kurumlara tavsiyelerde bulunmaktadır. Bu iki kuruluş, hükümetin bilgi güvenliği genel stratejisinin uygulanmasının genel gözetimini gerçekleştirmekte ve bilgisayar ağlarına ve elektronik ortamdaki işlemlere karşı olabilecek saldırılar konusunda erken uyarı işlevi görmektedir. Elektronik ortamdaki bilgi, belge ve işlemlerin güvenliğinin sağlanması amacıyla IT çözümleri geliştirilmesinin, temelde her bir kamu veya özel sektör kuruluşunun kendi sorumluluğunda olduğu kabul edilmektedir. Bu alanda önleyici işlev gören yazılım ve donanımların serbest piyasa koşullarında bu kuruluşlar tarafından temin edilmesi beklenmektedir.

Bu alandaki çalışmaların koordine edilebilmesi amacıyla "Chief Information Officer's Council" (CIOC) kurulmuş olup, ayda bir düzenli olarak toplanan sözkonusu Konsey'e CPNI ve CESG'e ilaveten silahlı kuvvetler ve istihbarat servisinin ilgili birimleri katılmaktadır. Buna ilaveten, daha kapsamlı eşgüdüm ihtiyacının karşılanması için "Information Assurance Policy and Programme Board" (IAPPB) ihdas edilmiştir. Kamu ve özel sektörle ilgili bilgi güvenliği politikası uygulamalarının ele alındığı sözkonusu Kurul, üç ayda bir toplanmakta ve toplantılara CIOC'a ilaveten Savunma Bakanlığı, Dışişleri Bakanlığı ve İş,

Girişim ve Reform Düzenlemeleri Bakanlığı'ndan yetkililer iştirak etmektedir.

Bilgi güvenliği konusunda İngiltere'de üç temel belge yürürlüktedir. Bunlardan "Transformational Government Agenda", çeşitli kamu kuruluşlarında görevli üst düzey IT uzmanlarından oluşan "Chief Information Officers' Council" ve teknolojik dönüşüm faaliyetlerinden kamu sektörünün azami ölçüde yararlanmasını sağlamakla yükümlü devlet görevlilerinden müteşekkil "Service Transformation Board" tarafından 2005 yılında dönemin Başbakanı Tony Blair'in talimatı üzerine hazırlanmıştır. Sözkonusu belge doğrudan bilgi güvenliğiyle bağlantılı olmayıp, İngiliz vatandaşlarının devlet kurumlarıyla gerçekleştireceği işlemlerde teknolojik imkanlardan azami ölçüde yararlanılmasını hedeflemekte ve bu amaçla gerçekleştirilecek çalışmaların esaslarını belirlemektedir. Bu çerçevede, bilgi güvenliği konusuna da değinilmektedir.

Bu alandaki çalışmalara ışık tutmak üzere ilk defa 2003 yılında hazırlanan rehber belge ise "Ulusal Bilgi Güvenliği Stratejisi"dir. Geçtiğimiz yıl tekonolojik gelişmeler ve bu kapsamdaki yeni ihtiyaçlar çerçevesinde güncellenen örneği ekli belgeyle, hükümet ve kamuoyunun çıkarlarını yakında ilgilendiren elektronik ortamda bilgi güvenliğinin sağlanması konusuna ilişkin genel ilkeler ve bu alanda İngiltere'de uygulamaya konulacak kurumsal yapı tespit olunmaktadır.

"Information Assurance Governance Framework" başlıklı belgede ise, bilgi güvenliğinin sağlanmasına riayet edilecek ulusal standartlar ve bu sorumluluğun ilgili kurumlar bünyesinde nasıl paylaştırılacağı ortaya konulmaktadır. Buna göre, İngiltere'de bilgi güvenliği alanındaki sorumluluk dağılımı şu şekildedir.

Kabine Sekreteri (Bakan düzeyinde) Edward Miliband: Başbakana karşı sorumludur. Bakanlık Müsteşarı (Permanent Secretary): Kabine Sekreterine karşı sorumludur.

Kıdemli Bilgi Riski Yetkilisi (Senior Information Risk Owner): Her bir kamu kuruluşunda yürütülen bilgi güvenliği çalışmalarından sorumlu üst düzey yetkilidir. Bakanlık Müsteşarına karşı sorumludur.

Bakanlık Güvenlik Yetkilisi (Departmental Security Officer): Kamu kuruluşları bünyesinde bilgi güvenliği politikası ve rehber ilkelerinin uygulanmasını gözetmek, meydana gelebilecek saldırıları rapor etmek ve araştırmakla yükümlüdür. Kıdemli Bilgi Riski Yetkilisine karşı sorumludur.

IT Güvenlik Yetkilisi (IT Security Officer): Bakanlık Güvenlik Yetkilisine yardımcı olmak üzere atanabilir.

I. İSVİÇRE

İsviçre'de elektronik ortamdaki tehdit unsurlarına karşı kontrol ve mücadele, türlerine göre farklı kurumlarca yürütülmektedir. Devlet kurumları, kamu kuruluşları ve ulusal güvenliği alakadar eden bilişim atakları ile mücadele hususunda görevli olan birim Federal Analiz ve Önleme Dairesi'dir ve bu kuruluş (DAP) sivil ve askeri istihbarat kapasitelerinden yararlanmaktadır. Federal İnternet Suçları ile Mücadele Koordinasyon Dairesi (CYCO) koordinasyonunda faaliyet gösteren Federal Polis Teşkilatı, elektronik ortamdaki bireysel ve örgütsel tehdit unsurlarının araştırması, takibi ve ele geçirilmesi çalışmalarını yürütmektedir.

İş dünyası ile münferit internet kullanıcılarının elektronik ortamdaki saldırılara karşı korunması, bilgilendirilmesi, olası saldırıların algılanıp karşı önlemlerin alınması ile yasal ve idari düzenlemelerin yapılması hususlarında Bilgi Güvenliği Analiz ve Bildirim Servisi (MELANI) sürekli araştırmalar yapmakta, gelen ihbarları ilgili birimlere yönlendirmekte ve yılda iki kez, ülke içi ve uluslararası internet güvenliği durum raporu düzenleyerek kamuoyunun bilgisine sunmaktadır.

İsviçre Hükümeti 1 Ekim 2004 tarihinden beri MELANİ servisini İsviçre'nin özellikle iletişim ve veri toplama hususundaki hassas kurumlarını korumak ile görevlendirmiş ve önlemler hususunda Zürih ETH üniversitesi ile müşterek çalışılmasını sağlamıştır.

Uluslararası elektronik ortam saldırıları tehditi ile mücadele konseptinde uluslararası işbirliğine ve özellikle ek değişiklik protokolünün yürürlüğe girmesinin ardından bu hususta etkinlik kazanan EUROPOL teşkilatı ile eşgüdüm içinde çalışılmasına önem verilmektedir.

Elektronik ortamdaki saldırılara karşı icra edilen faaliyetlerin konsept ve stratejisini saptayan üs kurulun adı Federal Enformasyon Stratejisi Kurumu ISB' dir.

İnternet sayfalarındaki güvenlik boşlukları, işletim sistemlerindeki zayıf noktaların tehlike arz etmemesi için hazırlanan güvenlik yamaları bir liste halinde Bilgi Güvenliği Analiz ve Bildirim Servisi (MELANI) web sitesinde yayınlanmakta, söz konusu yamalar buradan indirilerek bilgisayarlar daha güvenli hale getirilmektedir. Aynı şekilde internette yayınlanan ve şüpheli görülen web siteleri bu kuruma ihbar edildiğinde sayfa araştırılmakta ve sonucu halka duyurulmaktadır.

İ. İTALYA

İtalya'da Telekomünikasyon ve Bilgi İşlem sistemlerini kapsayan konular Telekomünikasyon Bakanlığı ile Yenilikler ve Teknoloji Bakanlığının yetki alanlarına girmektedir. Bu cihetle, telekomünikasyon ve bilgi işlem sistemleriyle ilgili ulusal kanunlar ve AB mevzuatı çerçevesinde Yenilikler ve Teknoloji Bakanlığı, Telekomünikasyon Bakanlığının mutabakatıyla, 16 Ocak 2002 tarihinde bir kararname yayımlayarak Kamu Sektörünün elektronik ortamlarda savunulması için Ulusal Güvenlik Komitesi kurulmasına karar vermiştir.

Sözkonusu iki Bakanlık 24 Temmuz 2002'de imzalanan müşterek bir kararname ile bahsekonu Ulusal Güvenlik Komitesi aracılığıyla uluslararası güvenlik standartlarına uyum ve risklere karşı konulması gibi gereksinimleri yanıtlayacak bilgi işlem ve telekomünikasyon güvenlik planları oluşturulmasında müşterek programlar izlenmesi konusunda da mutabık kalmışlardır. Yenilikler ve Teknoloji Bakanlığı ile ilintili sözkonusu komite beş kişiden oluşmaktadır. Başkan ve bir üye Telekomünikasyon Bakanlığı, diğer üç üye ise Yenilikler ve Teknoloji Bakanlığınca atanmaktadır.

Komitenin belli başlı görevleri arasında bilgi işlem güvenlik sistemlerinin uluslararası standartlara uyması için

proje ve öneriler hazırlamak, kamu kurumlarında güvenlik sistemlerinin oluşturulması için programlar oluşturmak, yapılan çalışmaları değerlendirmek ve gerektiği hallerde uyarılarda bulunmak, kamu personelinin güvenlik konusunda eğitimi için programlar hazırlamak gibi hususlar yer almaktadır. Komite her dört ayda bir yaptığı çalışmalara ve elde edilen somut neticelere ait bir rapor hazırlar ve bunları Telekomünikasyon Bakanlığına ve Yenilikler ve Teknoloji Bakanlığına göndermektedir.

Sözkonusu kararname kapsamında tüm kamu kuruluşları kendi bünyelerinde bilgi işlem güvenliği için bir birim oluşturmakla yükümlü kılınmışlardır. Komite ayrıca, "Computer Emergency Response Team" adlı bir birim oluşturmuştur. Sözkonusu birim içerisinde bilgi işlem hataları ve elektronik saldırılar konusunda kamu idarelerine destek vermek için özel bir birim bulunmaktadır (GovCERT). GovCERT „Computer Emergency Readiness“ görevi yapmakta ve her bir Kamu idaresi bünyesinde kurulan yerel birimlere destek vermektedir. Yerel Birimler, risk yaratan durumların çözülmesi ve savunma yazılımlarının güncelleştirilmesi konularında GOVCERT ile temas etmektedirler.

J. İSPANYA

İspanya'nın siber savunma politikasını CCN-STIC 001 "Bilgi Teknolojisi Güvenliği ve Kamu İdaresinde Gizli Ulusal Bilgiler İçeren Yazışmalar" belgesi kamu idari sistemlerinde kullanılan gizli bilgilerin doğru bir biçimde korunmasına ilişkin temel ilkeleri ve asgari gereklilikleri belirleyerek bu konudaki çerçeveyi oluşturur. . Kamu İdaresinde kullanılan sistemler için yasal çerçeve kısmen oluşturulmuş olup, uygulama kanalları ve kuralları belirlenmiştir. Bilgisayar sistemlerinde asgari güvenlik kurallarının belirlenmiş olduğu yetki kullanılan uygulamalarda bilgi güvenliği, kullanımı ve saklanması konusunda genel kriterler geçerlidir. Bu konuda uyulması gereken bir zorunluluk ya da denetim mekanizması bulunmamaktadır. 11 sayı ve 22 Haziran 2007 tarihli vatandaşların Kamu Hizmetlerine elektronik ortamda erişimine ilişkin yasa uyarınca Kamu İdaresinde kullanılan sistemlerinde kullanılacak temel ilkeler ve asgari gereklilikleri oluşturmayı amaçlayan Ulusal Güvenlik Şeması geliştirilme aşamasındadır. Stratejik önem arz eden altyapı şirketlerinin sistemleri için bir düzenleme halihazırda bulunmamaktadır. Bununla beraber 2007 yılında İçişleri Bakanlığı, Güvenlik Devlet Sekreterliğine bağlı Stratejik Önem Taşıyan Altyapıları Koruma Ulusal Merkezi (CNPIC) stratejik açıdan ulusal önem taşıyan altyapıların güvenliğinin sağlanması konularını koordine eden bir organ olarak kurulmuştur. Bu merkezin görev alanına giren sektörlerden biri de Bilişim Teknolojileri sektörüdür. CCN, tüm devlet kurumları (merkezi, özerk, yerel) ile işbirliği yapmak ve onlara yardımcı olmakla görevli ulusal uyarı merkezi konumundaki CCN-CERT aracılığıyla doğabilecek güvenlik sorunlarına hızlı ve etkili bir biçimde çözüm bulmayı ve günümüz şartları içinde doğan yeni tehditlerle etkin şekilde mücadele etmeyi hedeflemektedir. Siber savunma politikası, halihazırda sadece devlet kurumlarının sistemlerini kapsamaktadır. Sanayi Bakanlığı tarafından Telekomünikasyon hizmeti veren şirketler için belirlenen yasal engellemeler ve idari gerekliliklere ilişkin uygulama hariç devlet kurumlarınınkiler dışında kalan sistemler için yasal düzenleme mevcut değildir.

K. TÜRKİYE

Ülkemizde ise konuyla ilgili doğrudan bir çalışma bulunmakla birlikte konunun bir düzene bağlanmasına yönelik genel nitelikli kurumsal ve mevzuat anlamında bir dizi çalışmalar yapılmıştır. 15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu, 4 Mayıs 2007 tarihli ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi hakkındaki kanun konuyla ilgili düzenlemelerdir. 5651 sayılı kanun internet ortamında işlenen suçları sekiz ayrı kategoride değerlendirmekte, bilgi güvenliği, siber terörizm gibi suçlara yer vermemektedir. E-dönüşüm Türkiye Bilgi Toplumu Strateji Belgesinin Eylem Planında ise 88 numaralı eylem Ulusal Bilgi sistemleri Güvenlik Programı olarak belirlenmiş ve 2008 Aralık ayına kadar tamamlanması amacıyla TÜBİTAK-UEKAE görevlendirilmiştir.

IV. STRATEJİLERİN VE ÜLKELERİN DEĞERLENDİRİLMESİ

Bu çalışma kapsamında, ABD, Almanya, Danimarka, Finlandiya, Fransa, Güney Kore, İngiltere, İspanya, İsviçre ve İtalya'daki siber saldırılara karşı savunmaya yönelik ulusal anlamda yapılan hazırlıklar, kurumsal düzenlemeler, hazırlanan yasal mevzuatlar açıklanmıştır. Ülkelerdeki çalışmalar genel olarak incelendiğinde;

- Siber savunma konusunda ülkelerin tamamının duyarlı ve tehlikenin farkında olduğu,
- Konu ile ilgili yasal düzenleme yoluna giden ülkelerin çoğunlukta olduğu, bazılarında ise düzenleme olmasına rağmen yasal zorunluluk getirilmediği,
- Ulusal anlamda siber savunma sorumluluğunun bazılarında bağımsız bir organa verilmesine rağmen bazılarında Bakanlıklar düzeyinde çok sayıda kurumun sorumluluğuna dağıtıldığı,
- Ülkelerin tamamında hazırlık olmasına rağmen olası bir saldırı durumunda atılması gereken adım konusunun açıklığa kavuşturulamadığı,
- Herbir ülkenin tamamen farklı yöntem ve stratejilerle konuya yaklaşım sergileyebildikleri,
- Ülkemiz gelişmiş ülkelere göre yapılan düzenlemeler ve kurumsallaşmalar bağlamında geri kaldığı, gereksinimlerin karşılanmasına yönelik adımların hızlandırılmasında yarar olacağı

değerlendirilmektedir.

KAYNAKLAR

1. The National Strategy to Secure Cyberspace
2. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
3. http://www.dhs.gov/index.shtm
4. İç Güvenliğe ilişkin Başkanlık Direktifi www.whitehouse.gov/mews/relases/2003/12/20031217-5.html
5. IT- security Beyond Borders http://www.tekno.dk/pdf/projekter/it-sec2007/2007_it-security-across-borders-summary.pdf
6. Creating a Safer Information Society www.mintc.fi/scripts/cgiip.exe/WService=lvm/cm/pub/showdoc.p?docid=2433&menuid=431
7. http://www.telecom.gouv.fr/fonds_documentaire/rapports/cybercriminalite.pdf
8. Korea Information Security Agency-www.kisa.or.kr
9. Korea Internet Security Center-www.krcert.or.kr
10. Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency) http://www.enisa.europa.eu/index.htm
11. http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2008/0097
12. http://www.csae.map.es/csi/pg3428.htm
13. E-Dönüşümde Türkiye Nerede? Y. Turan Çetiner, Uluslararası Ekonomik Sorunlar Dergisi, T.C. Dışişleri Bakanlığı, Kasım 2008