

ULUSAL BİLGİ GÜVENLİĞİ RAPORU VE TEKNOLOJİK GELİŞMELER

Erkut ERSOY

Ulusal Bilgi Güvenliği Raporu ve Teknolojik Gelişmeler

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler yeni bir çağ yaratmıştır. Bilgi çağı olarak adlandırılan bu çağda ekonomide ve sosyal yaşamda klasik paradigmlar yetersiz kalmakta; teknolojik gelişmeler yeni yapılar, yaklaşımlar yaratmaktadır. Bu nedenle, bilgi güvenliğine ilişkin ulusal bir politika oluşturmanın temel koşullarından birisi, bilgi ve iletişim teknolojilerinde gözlenen gelişmelerin bilinmesidir. Bu noktada, söz konusu teknolojik gelişmelerin ne olduğunu ve ne yönde olacağını doğru anlamak ve içeriğini doğru belirlemek son derece önemlidir:

Kriptoloji, internetin yaygınlaşması ve bir ticaret medyası haline almaya başlamasıyla, bilgi güvenliğinin sivil uygulamalarına tanık olmaya başlamıştır. Bu uygulamalar kısaca "açık anahtarlı altyapılar (Public Key Infrastructure-PKI)" olarak isimlendirilebilir. Açık anahtarlı altyapılar, bir gizli ve açık anahtar çifti ve bu çiftle sağlanan "elektronik kimlik, sayısal imzalama ve şifreleme" işlevleriyle, gerekli kurumsal ve yasal yapılanma üzerine kurulmuştur. Burada şu noktalar önemlidir:

Kripto işlemleri donanım üzerinden yazılıma kaymıştır. Örneğin kripto teçhizatı, saklanması, imhası ve benzeri unsurlar bu altyapıda karşılaşılan ve kullanılan terimler değildirdir.

Söz konusu yazılımlarda kullanılan algoritmalar tümüyle kamuya açıktır. Bunun anlamı, bu algoritmaların çok sayıda taraf tarafından testinin yapılabilir olması ve bu yolla güvenilirliğinin artmasıdır.

Anahtarların üretilmesi, saklanması ve tüm işlevlerin yürütülmesi için uluslararası açık standartlar belirlenmektedir (X.509 elektronik kimlik belgesi standardı, PKCS açık anahtarlı altyapılar standartları gibi). Bu standartların dışına çıkmak pratik değildir.

Açık anahtarlı altyapıların gerektireceği yasal düzenlemeler de, (onay kurumlarının yapılandırılması, sayısal imzanın kabulü, vb.) uluslararası uyumun gereği olarak yerine getirilecektir.

Konu ile ilgili ilk yasa ABD'de Utah eyaletinde kabul edilmiştir (1995). Bunu Almanya (1997) ve Singapur (1998) sayısal imza yasaları izlemiştir. Halen Avrupa Topluluğu üye ülkelerinde böyle bir yasa için çalışmalar sürmektedir. Genel eğilimlerin dışında geliştirilmeye çalışılacak uygulamalar sosyal ve ekonomik açıdan zararlı olabilecek, uluslararası standartlara uymayan yapılanmalar ülkeleri yalnızlığa itecektir.

İnternet yalnızca bir iletişim altyapısı değildir. Kimi yorumlara göre bilginin yaratılması ve paylaşılması için bir "özgürlük ortamı" anlamına da gelmektedir. Gerçekten de internet sınırsız bilginin yayılmasının medyası olmuştur. Bu bağlamda, kriptografik ürünler hızla ve kolaylıkla yayılabilmektedir. Bu durum, ABD'deki aksi yönde gayretlere karşın değişmemiş aksine gelişmiştir. Örneğin, ABD tarafından sınırlandırılmış pek çok ürünü, ABD üzerinden ya da dünyanın başka bir köşesinden internet aracılığıyla edinmek "teknik olarak" son derece kolaydır. "Teknik yöntemlerle" bunun önüne geçilmesi olanaksızdır. Dolayısıyla, "İnternetteki bu durumun denetlenmesi" amacıyla yapılacak girişimler "teknik açıdan geçersizdir". Bunun yanında şu noktalar da dikkat çekicidir:

İnternet protokolü IP'nin gelecekteki versiyonu IP v6, IP düzeyinde "şifreleme" sağlayacaktır. Bu durumda anahtarların saklanması da olanaksızlaşacaktır.

Bilgi ve iletişim teknolojilerinde, ulusal devlet politikaları "teknolojik yansızlık" ilkesini benimsemişlerdir. Bunun anlamı kamunun, gelişme aşamasında bir teknolojiyi diğerlerine üstün saymaması ya da tercih etmemesidir. Diğer bir deyişle, teknolojilerin açık rekabet ortamında birbirlerine üstünlüklerinin sağlanmasıdır.

Bütün bu teknolojik gelişmeler göz önüne alındığında oluşturulacak politika ilkelerinin ve kurumsal yapılanma önerilerinin, ileride sorunlar yaratabilecek uygulamalardan kaçınılması gerektiğini göstermektedir. Yukarıda sözü edilen teknolojik tarafsızlık ilkesi, teknolojik açık rekabet ortamının sağlanması gibi konular göz önüne alındığında oluşturulacak politikaların bunlarla çatışmaması gerekmektedir. IP v6 ve sonrası gelişmelerin ışığında, teknik açıdan gerçekleştirilemeyecek görevler, kurumsal önerilerde yer almamalıdır. Bu nedenle, gelişmiş ülkeler bu yeni gelişmelere karşı tedbirler almak konusunda çok temkinli davranmaktadırlar. Mevcut yasalarla sahip oldukları yetkileri de, kullanım alanlarına açıklık getirerek sınırlamaktadırlar.

Diğer Ülkelerdeki Durum

Birkaç yüzyıllık geçmişi olan demokrasinin, çağımızda ortaya çıkan çok yoğun bilgi transferi ihtiyacına ayak uydurmasını sağlayacak arayışlar sürmektedir. Demokratik ülkeler, kriptografik yazılım ve donanım kullanımı söz konusu olduğunda kişisel/ticari özgürlüklerle ve devlet/kamu güvenliği arasında bir denge bulmaya çalışmaktadırlar. Bilgi güvenliği, uzun yıllar boyunca ve özellikle Soğuk Savaş döneminde, askeri ve diplomatik haberleşmenin önemli bir parçası olarak ele alınmıştır. Bu açıdan bakıldığında kavram, bilginin güvenli iletimi kadar, "hasım ulusların" elektronik istihbarat yöntemleriyle dinlenmesi olarak anlaşılmıştır. Özellikle gelişmiş uluslar, bu amaçlarla Soğuk Savaş döneminin hemen başlarında çeşitli kurumlar ihdas etmişlerdir.

Gelişmiş ülkelerdeki gelişmeler aşağıda özetlenmiştir.

ABD

Kişisel özgürlüklerin zedelenmemesi prensibinin neredeyse anane haline geldiği bu ülkede, devlet, yurttaşlarının haberleşmenin mahremiyeti konusunda hakları ile terörizm, kaçakçılık ve devlete karşı işlenen diğer suçların önlenmesi konusunda dengeleri de kurmuş bulunmaktadır. ABD'de 1952 yılında kurulan "Ulusal Güvenlik Teşkilatı (National Security Agency)" bu dengenin içinde kendine özgü bir yere sahiptir. NSA, ABD çıkarları doğrultusunda bir yanda uluslararası elektronik istihbarat yapmak ve öte yanda Amerikan devletinin bilgi güvenliğini sağlamaktan sorumludur. NSA, uzman teknik fonksiyonları sağlamaktan sorumlu kılınan Savunma Bakanı'nın yetki, kontrol ve yönlendirmesinde ve Savunma Bakanlığı bünyesinde bağımsız bir teşkilat olarak kurulmuştur.

NSA'nın günümüzde aldığı biçim hakkında şu noktalar önemlidir:

NSA, tam olarak bir "elektronik istihbarat" örgütüdür. Hatta bu öyledir ki; NSA "ABD İstihbarat Topluluğu (US Intelligence Community)" içinde, CIA, FBI, "Ordu İstihbarat (Army Intelligence)" ve Savunma Bakanlığı gibi toplam 13

federal kurumdan birisidir ve bu kuruluşundan beri değişmemiştir. Ayrıca, 1972 yılında kurulan "Merkezi Güvenlik Birimiyle (Central Security Service)" NSA ve ordu istihbarat birimleri arasında tam bir işbirliği sağlanarak Savunma Bakanlığının kriptografik çalışmaları tek bir bünyede verilmeye başlanmıştır. (1)

NSA "diğer uluslar ve onların tarafları için istihbarat ve karşı istihbarat" in istihbarat etkinlikleriyle sınırlıdır. Amerika'da oturma izni olan yabancılar, Amerikan vatandaşları ve Amerikan özel sektör kurumlarının gizlilik haklarına aykırı yasadışı istihbarat yürütmesi anayasa ve NSA'in kuruluş yasasıyla kesinlikle yasaklanmıştır. Bunun ötesinde, gizlilik ve haberleşme özgürlüğü yasalarıyla kişiler kendileri hakkında NSA gizlilik yasasında tanımlanan "kimlik bilgilerine" erişme hakkına sahiptirler. Haberleşme özgürlüğü kapsamına giren "hükümet kayıtlarının" NSA tarafından tutulması yasayla engellenmiştir. (2)

NSA "ithalat ve ihracat politikalarının" belirlenmesinde görevli değildir ve kendi dışında oluşan politikalara tabiidir. ABD'de bu politikalar "Başkanlık" düzeyinde saptanır.

NSA'in ABD'deki "kriptografi üretimini" kontrol altında tutmak, söz konusu ürünleri sertifikalandırmak türünden hiçbir işlevi ve görevi yoktur. Hatta, özel üreticiler kamuya ürünlerini satarlarken dahi, NSA'in onayını almak zorunda değildirlir. Tam aksine, NSA, gelişmiş yeteneklerinden ABD özel sektörünün de yararlanmasını sağlamak amacıyla, özel sektörün isteğine bağlı olarak danışmanlık vermektedir. (3)

Kamuda bilgi güvenliği standartlarının belirlenmesi ve uygulanması da NSA'in görevleri arasında değildir. ABD'de bu işlevi, Amerika Standartlar Enstitüsü (National Institute of Standarts and Technology) "Federal Bilgi İşleme Standartları (Federal Information Processing Standarts)" yayınlarıyla yerine getirmektedir. Bu bağlamda Madde 8'in çeşitli bentlerinde ve farklı biçimlerde tekrar edilen "usuller ve yöntemler belirlemek, altyapıları korumak" fiilleriyle ifade edilen ve temelde kamuda bilgi güvenliği standartlarının altyapılar, ürünler ve uygulamalar açısından saptanmasına dönük olduğu anlaşılan işlevler bu kapsama girmektedir.

1993 yılı Nisan ayında Clinton yönetimi NSA tarafından hazırlanan/önerilen yeni bir kriptoloji politikasını ortaya koymuştur. Başkan Bush zamanından başlayarak yürütülen bu çalışmaların odak noktası hükümet tarafından geliştirilen Clipper adlı bir kripto çipidir. Özel sektör tarafından üretilen her türlü güvenli iletişim ürünlerine yerleştirilmesi önerilen bu çipe karşı çok büyük bir tepki oluşmuştur. Bu tepkilerin kaynağında, her çip için özel olarak üretilen anahtarların bir kopyasının hükümet tarafından tutulması ve tamamen yasal olmayan hiçbir nedene dayanarak bu çipler üzerinden geçen trafiğin dinlenmeyeceğinin hükümet tarafından garanti edilmesine rağmen, yeterli güvenin oluşturulamaması bulunmaktadır. Ayrıca, hükümet tarafından geliştirilen anahtar algoritmasının açıklanmaması sonucunda algoritmanın denenmesinin ve güvenilirliğinin kanıtlanamayacak olması, bunun sonucunda tüketicilerin bu ürünlere rağbet etmeyeceğinin ortaya çıkması, gittikçe önem kazanan kriptoloji sanayiinde dünya pazarlarında rekabet şansının kapalı bir algoritma kullanılarak üretilen ürünlere dayanarak korunamayacağı gibi endişeler ortaya çıkmış ve bu çip istenen kullanım yaygınlığına ulaşamamıştır. (4)

Öte yandan "yaşamsal altyapıların korunması" (critical infrastructure protection) yeni bir kavram olarak dünya ülkelerinin gündemine girmiştir. Yaşamsal altyapıların korunması kavramı, ekonominin ve devletin minimum düzeyde

işleyişi için gerekli fiziksel ve ağısal sistemleri kapsamaktadır. Amaç, ülkenin düşmanlarının, bunlar ister başka ülkeler, ister ülke içindeki gruplar ve bireysel olsun, "geleneksel olmayan" yöntemlerle yapacakları saldırıların engellenmesidir. Açık ki, bu tehditler, devletin elektronikleşmesi ve açık ağları kullanmasının yaygınlığıyla doğru orantılıdır. Yaşamsal altyapıların korunması için ABD Başkanı Bill Clinton, 1998 yılında bir Beyaz Belge direktifleri yayınlamıştır. Bu belgede dikkat çeken unsurlar şunlardır:

Devlet içinde öncü kurumlar tespit edilmiştir. Her öncü kurum çeşitli sektörleri paylaşmışlardır. Örneğin, Ticaret Bakanlığı iletişim ve enformasyon sektörüne; Hazine Bakanlığı bankacılık ve finans sektörüne, FBI polis, acil durum ve adalet konularına; CIA dış istihbarata; Dışişleri Bakanlığı dışişleri sektörüne; Savunma Bakanlığı savunma sektörüne liderlik edecek kurumlar olarak belirlenmişlerdir. Ayrıca, Bilim ve Teknoloji Politika Genel Müdürlüğü, Ulusal Bilim ve Teknoloji Konseyi'nin programları aracılığıyla araştırma ve geliştirme çalışmalarını eşgüdümlemekle görevlendirilmiştir. Öncü kurumların seçilmesinin nedeni, bu konuda, özel sektör/kamu sektörü işbirliğini gerektirmesi ve gereksiz hükümet düzenlemeleri yaratmaktan kaçınılmasıdır.

Ulusal Eşgüdümcü: Güvenlik, Altyapı Koruma ve Karşı-terörizm Ulusal Koordinatörü bu direktifin eşgüdümünden sorumludur.

Uyarma ve Bilgi Merkezleri: Başkan, bu görevle FBI'ya sorumlu kılmıştır.

National Infrastructure Protection Center (NIIPC): Bu heyet, FBI, bilgisayar suç uzmanları, Savunma Bakanlığı, İstihbarat topluluğu ve önder kurumların temsilcilerinden oluşur. (5)

İngiltere ve Almanya

NSA dışında gelişmiş ülkelerden anılan iki diğer örnek kurum İngiltere'deki Kamu Haberleşmesi Koordinasyonu (Government Communications Headquarters) ve Almanya'daki Enformasyon Teknolojileri Güvenlik Kurumudur (Bundesamt für Sicherheit in der Informationstechnik). İngiltere'deki Kamu Haberleşmesi Koordinasyonu (Government Communications Headquarters), NSA'ya çok yakın işlevler yürütmektedir. GCHQ'nun da oluşumu Soğuk Savaş dönemine dayandırılmaktadır. (6)

Enformasyon Teknolojileri Güvenlik Kurumu (BSI) ise NSA ve GCHQ örneklerinden farklı olarak, istihbarat işlevi olmayan bir kurumdur. BSI bir Alman kamu kurumu olarak, bilgi ve bilgisayar sistemleri güvenliği konularında araştırma yürüten bir kurumdur. Araştırma sonuçları, kamuda söz konusu güvenlik uygulamalarının yapılmasına yarar sağlamaya çalışmaktadır. Kurum adli olaylarda da emniyete talep olduğu takdirde danışmanlık hizmeti verebilmektedir. (7)

Alman Hükümeti de söz konusu teknolojiyi yasaklamak üzere girişimlerde bulunmaya başlamıştır. 4 Mayıs 1995 tarihinde Alman Parlamentosu "Telekomünikasyon İzleme Kanunu" adı altında ülkede tasarlanan ve kullanılan telefon, GSM, ISDN ve bilgisayar şebekesi tarayıcılarının, devlet birimleri tarafından gerektiğinde dinlenmesini sağlamak için standart bir ara bağlantı sağlamaları konusunda bir kanun teklifini onaylamıştır. Kanunun özünü, güçlü delillere dayanarak bağımsız bir yargıç kararı olmadan özel haberleşmenin dinlenememesi oluşturmaktadır. Yargıcın

gerekli gördüğü durumlarda, bu kanuna göre çağrı oluşturma bilgilerine ve GSM kullanıcılarının hücreler arasında izlenmesini sağlayacak bilgilere erişilmesi mümkün hale gelmektedir. Almanya, bu düzenlemesiyle, Avrupa ülkeleri arasında bireyi devlete karşı üst düzeyde güvenceye alan bir ülkelerin öncülüğünü yapmaktadır.

Norveç

Norveç'te kriptografik ürünlerin yurt içerisinde kullanımında herhangi bir yasaklama yoktur ve ithalatında da kontrol bulunmamaktadır. (8)

Norveç Wassenaar anlaşmasının bir üyesidir ve bu bağlamda kriptografik ürünlerin ihracatını 1987 tarihli bir yasayla kontrol etmektedir. İhracat kontrolü Dışişleri Bakanlığı'nın sorumluluğundadır. Norveç yasaları Wassenaar anlaşmasında yer alan genel yazılım istisnasını gözetmektedir. Ayrıca, internetin genel yazılım notunun uygulanması ve kriptografik ürünlerin iletilmesi için yeterli bir temeli teşkil ettiği benimsenmektedir.

Norveç'te yürütülmekte olan Kamu Sektörü Ağ Projesinde, sayısal imza sayısal kimlik belgesi ürünlerinin oluşturulması hedeflenmektedir. Bu projenin "açık anahtarlı altyapılar" (PKI) için yasal, teknik ve organizasyonel düzenlemeler için deneme olduğu ve temel teşkil edeceği planlanmaktadır.

SEIS–Secure Electronic Information in the Society, kamu ve özel sektör örgütlerinin ortaklaşa çalıştığı bir gruptur. Elektronik kimlik kartları için kamuya açık standart geliştirmişlerdir. (PAS) Norveç ulusal standartlar kurumu SEIS temelli İsveç standardını Norveç ulusal standardı olarak kabul etmeyi planlamaktadır. (9)

Norveç, bir dizi şifreleme sisteminden oluşan ve çalınamaz biçimde silisyuma yazdığı NSK adlı milli algoritma yazmıştır. NSK (Norwegian standart for cryptography) algoritmasını kullanan NX1000 gibi kriptografik cihazlar Norveç pazarında bulunabilmektedir.

ABD'de kriptografik teçhizat Wassenaar ilkeleri gereğinde "mühimmat" gibi görmektedir. "Mühimmat kavramı" askeri bir terim olarak, kriptografik ürünlerin, 1998 Wassenaar düzenlemesinde, "askeri ve ticari olmak üzere çift kullanımlı" teknolojilerden sayılmaya başlanmasıyla ilgilidir. Bunun anlamı, bu düzenlemeye imza koyan ülkelerin, kriptografi ürünlerinin ithalat ve ihracatında "uyumlu" politikalar izleme niyetinde olduklarıdır. Ancak Wassenaar bir anlaşma değildir ve yaptırım yoktur. Nitekim, İsviçre hükümeti 1998 düzenlemesinin "liberal politikalarında" bir değişikliğe neden olmayacağını ve İsviçre firmalarının dünya pazarından en yüksek payı almaları konusundaki desteğinin devam edeceğini açıklamıştır (Bkz. Cryptography and Liberty 1999, EPIC). Wassenaar üyesi İrlanda ise, en başından beri ABD ve İngiltere'nin aksi yönünde politikalar izlemiştir. İrlanda'nın bir firması olan "Baltimore Inc." bugün dünyanın en önde gelen bilgi güvenliği firmalarından birisidir.

ABD, 1998 Wassenaar düzenlemesinin aksi yönünde, ihracat politikalarını 2000 yılıyla beraber değiştirmiştir. Wassenaar 1998 açık bir biçimde internet tarayıcılarında 56 bit anahtar uzunluğunda kriptoya izin verirken, ABD bu yılın başından itibaren 128 bit anahtar uzunluğunu ihracat etmeye başlamıştır. ABD kökenli web sunucuları da paralel bir biçimde 128 bit SSL destekler bir biçimde ihracat edilmeye başlanmıştır. Ülkemizde bazı bankaların internet sayfalarında bu konunun uygulanması görülmektedir.

Bu deęişimde, "ticari çıkarların" ağır bastığı vurgulanmaktadır. Deęişiklik, tümüyle liberal bir politika deęilse de, geçmiş uygulamalara göre liberalleşme anlamına gelmektedir. (10)

Fransa'da da kriptografik yazılım ve donanım "mühimmat" olarak tanımlamakta ve işlem görmektedir. Yasa ile kriptografik teçhizatın ihracatı ve kullanımı devlet denetimine tabi kılınmıştı. Bir süre, Fransa'da faaliyet gösteren yabancı şirketler "ulusal güvenlik" nedeni ile kullandıkları anahtarları Fransız hükümetine bildirmek zorunda kaldılar. Ancak daha sonra bu politikalardan vazgeçilmiştir. Almanya, Finlandiya ve İtalya en başından beri liberal politikalar izlerken, Fransa 1999 yılında gösterdiği deęişimle ilginç bir uyum örneęi sergilemiştir. Fransa'da da artık sadece "beyan" yöntemi uygulanmaktadır. Gerçekten de Fransa yakın zamana kadar, "sertifikalandırma" yöntemiyle ihracat ve ithalatı kontrol altında tutmaya çalışırken, 1999 yılı başında Başbakan'ın birinci ağızdan açıklamalarıyla sadece ticari politikalarında deęil ancak tüm ulusal politikalarında önemli deęişikliklere gittiğini duyurmuştur. (11)

Avrupa Birlięi, dięer ulusal politika konularında olduęu gibi, ihracat ve ithalat izinlerinde de ABD'ye oranla çok daha liberal politikalar izlemektedir. Son olarak, 22 Mayıs 2000 tarihinde Lizbon'daki Dışışleri Bakanları toplantısında onaylanması beklenen bir düzenlemeyle, kriptolojik ürünlerin ihracatına getirilen sınırlamalar büyük ölçüde kaldırılacaktır. Bu düzenlemeyle, ihracat yapacak firmaların, ürünün son kullanıcısının Avrupa Birlięi ülkelerinde veya aralarında Kanada, Japonya, ABD, Avustralya ve Yeni Zelanda'nın da bulunduęu 10 ülkeden birinde bulunduęunu beyan etmeleri yeterli olacaktır. Avrupa Birlięi ve adı geçen dięer ülkeler bu alanda dünya pazarının % 80'ini oluşturmaktadırlar.

Bu hamleyle, AB ülkeleri firmaları bu pazarda özellikle ABD'li firmalara karşı büyük avantaj sağlamış olacaktır. Bu nedenle, çok yakında ABD'li firmaların hükümete baskı yaparak kendi ülkelerinde de benzer bir düzenlemenin yapılmasını istemeleri beklenmektedir.

OECD'nin 1998 yılında gerçekleştirdięi "Kriptografi Teknolojilerindeki Kontroller" başlıklı envanter çalışmasının raporu 1999 yılında yayınlanmıştır. Bu envantere göre kriptografik ürünlerin ihracat ve ithalatından sorumlu kurumlar büyük çoęunlukla ekonomiden ya da sanayi ve ticaretten sorumlu bakanlıklardır. Envantere göre yalnızca Avustralya ve Türkiye'de sorumlu bakanlıklar olarak Savunma Bakanlıkları belirtilmiştir. Türkiye'de ayrıca Dış Ticaret Müsteşarlığı da sorumlu kurum olarak belirtilmektedir. (12)

Türkiye'de Durum

Ulusal Güvenlięi ilgilendiren bilginin örgütlenmesi açısından, "gizlilik dereceli" bilginin ne olduęu, nasıl üretileceęi, korunacaęı, nakledileceęi, kullanılacaęı ve imha edileceęi konusunda T.C. Devleti'nin yasal hazırlığı ve düzenlemesi bulunmamaktadır. Bu yasal düzenlemeler ise geçici olarak kurulup sonra dağıtılan birtakım platformların üstesinden gelebileceęi gibi basit bir yasa ya da mevzuat deęil, çok karmaşık bir yasalar zinciridir ve gelişen teknoloji nedeni ile sürekli güncellenmek ve teknolojiye uygun hale getirilmek zorundadır.

Ulusal bir bilgi güvenlięi politikasının olmayışı ülkenin ulusal güvenlięini hassas hale getirmektedir.

Bakanlıklar, kamu kurum ve kuruluşları arasında ulusal güvenlik ihtiyaçları doğrultusunda bilgi güvenliğini koordine edecek, yönlendirecek ve ulusal bilgi güvenlik sistemini işletecek bir yapı yoktur.

Ulusal bilgi güvenliği gibi karmaşık ve konunun nasıl çözülebileceği hususunun müzakere etmek için ortak anlayışı kolaylaştıracak, üzerinde mutabakata varılmış tanımlar mevcut değildir.

Hassas bilgi altyapısına bağımlılık ve bu altyapıya tehdit ve riskler, kurum ve kuruluşlarca iyi anlaşılammıştır.

Kriptografik ürünlerin ithalatı ve ihracatı ile ilgili kontrol esasları net olarak belirlenmemiş olup kontrol mekanizması tam olarak tesis edilememiştir.

Politika Açısından

- ◆ Kamu kurum ve kuruluşlarında ulusal kullanım amaçlı onaysız hiçbir kripto cihazının kullanılmaması,
- ◆ Ulusal kriptoloji politikasının, icra ve yasama organları tarafından geliştirilmesi,
- ◆ Kriptoloji üzerindeki icraat kontrolünün, dış ticareti arttıracak ancak ulusal savunma gereklilerini dikkate alacak biçimde tespit ve uygulanması,
- ◆ Devletin, özel sektörde de, gelecek talep üzerine bilgi güvenliğini geliştirecek mekanizmalarının kurulmasını teşvik etmesi ve desteklemesi,
- ◆ Haberleşme ve bilgi sistemleri ile kripto teçhizatının milli imkanlarla yurtiçi kaynaklardan sağlanması,
- ◆ Bilgi teknolojilerinin gelişimi için Araştırma–Geliştirmenin devletçe desteklenmesi gerekmektedir.

Sonuç ve Değerlendirme

Kriptolojik ürün geliştirme tek başına bir sanayi olarak görülmelidir. Bu konuda uygulanacak akıllı politikalarla bu tür ürünler ülkemiz için önemli bir ticari meta haline gelebilir. Ayrıca birkaç yıl içinde geliştirilen her yazılım için o yazılıma özgü kriptolojik bir modül olabileceği gibi, internet sayfalarındaki erişim de kriptolojik yöntemler içerebilecektir. Bütün bu muhtemel gelişmeler kriptolojinin artık bir ticari ürün olduğunu ortaya koymaktadır. Bu tür ürünlerin geliştirilmesine konulacak kısıtlar ülkemizdeki herhangi bir ticari ürünün geliştirilmesine karşı konulmuş kısıt gibi, ticari iş hacmini engelleyecektir.

Ayrıca, konu uzmanlarından London School of Economics akademisyenlerinden Stuart J.D. Schwartzstein tarafından da belirtildiği gibi, gizli anahtarın elde edilmesi, ve güvenilir üçüncü tarafta tutulması gibi çalışmaların önümüzdeki dönemde politik, ekonomik ve teknik nedenlerden dolayı başarılı olması beklenmemektedir. (13)

Kanunun bu yanları da düşünüldüğünde, ulusal politikalar açısından yeni kurumsal ve yasal yapılanmanın aşağıdaki ilkeleri de göz önüne alması gerekmektedir:

"Ulusal bilgi güvenliğini sağlamaya ilişkin bilginin" tanımı belirli olmalıdır. Ters durumda, belirsiz tanım altında, kamu ve özel kurumlarda bilgiye "Ulusal Bilgi Güvenliği Teşkilatı" tarafından erişme hakkı tanınmış olur ve gereğini yapmayan kamu ve özel kurum sorumlularına hapis cezası öngörülebilir. Bu durumun yukarıda özetlenen eğilimlerle ve dünyadaki durumla taban tabana zıt olduğu açıktır.

"Anahtarlama materyalinin üretim esaslarını" hangi durumlar ve koşullar altında belirlenmesinin geçerli olduğu açık olmalıdır. Burada "kişilerin gizli anahtarlarının" yasa kapsamı dışında olduğu açıkça belirtilmelidir.

Kamu ve özel kurum üreticilerini sertifikalandırma yoluna gidilmemelidir. Daha önceden de sözü edildiği gibi, sertifikalandırma ihracat ve kimi yerlerde de kamuya satımlarda uygulanan bir yöntemdir. Yine açıklandığı gibi, bu uygulamalar yok olmaya başlamıştır ve sadece ihracat ve ithalat için "beyan usulüne" geçilmiştir. Bu maddede sadece kamu alımları öngörüyorsa bu açıkça ifade edilmelidir. O durumda dahi, aşağıda ifade edilecek sakıncalardan uzak durulması gereği göz önünde bulundurulmalıdır.

"Ulusal Bilgi Güvenliği Teşkilatının" işlevleri ve ilgi alanı netleştirilmelidir. Bu teşkilatın aynı anda bir istihbarat örgütü, bir araştırma-geliştirme kurumu, bir standartlar enstitüsü, bir ürün sertifikalandırma kurumu, bir kamu düzenleme kurumu olmadığı açıkça belirtilmelidir.

Bu bağlamda "ulusal bilgi güvenliği", "ulusal güvenliği ilgilendiren bilgi" tanımları belirsizlikten kurtarılmalıdır. Bu açıdan bakıldığında Devlet Haberleşme ve Bilgi Teşkilatı altında örgütlenmek daha uygun olabilir.

Kurum yukarıda sayılan işlevlerden hangisine evrilirse evrilsin, özel kişi, kurum ve kuruluşlar kapsam dışında tutulmalıdır. "Özel kişi ve kurumlarla" ilgili hükümler koyulmamalıdır.

Yasa haksız rekabet ve tekelleri uygulamalara yol açabilecek, teknolojik açık rekabet ortamını zedeleyecek bir yapılanmadan arındırılmalıdır. Buna göre, özel sektörün üretiminin denetimi söz konusu olmamalıdır. Kamu alımlarında, teknolojik tercih dayatmasına gidilemeyeceği açıkça beyan edilmelidir.

Ticari politikalar, kişisel ve ticari gizlilik hakları tümüyle ulusal politikalar düzeyinde ele alınabilecek konulardır. Bu bağlamda kararlar "siyasi otoriteye" bırakılmalıdır. Kurumsal yapı, ancak talep olduğunda danışmanlık veren bir kurum statüsünde olmalıdır. Yasanın bu konudaki ilgili maddeleri değiştirilmelidir.

Bilgi güvenliğinin sivil uygulamaları dünyada henüz çok yenidir. Ülkemizde de bilgi teknolojilerinin gelişmişlik düzeyi üretim, tüketim ve içerik açısından gelişmiş ülkelerin çok altındadır. Bu iki gerçek, bilgi güvenliğinin sivil uygulamalarında bir düzenlemeye gitmek için henüz çok erken olduğunu göstermektedir. Bu bir yana, bu düzenlemeleri yukarıda da ifade edilmeye çalışıldığı gibi kapsamı ve işlevleri belirsiz bir kurum marifetiyle yapmaya çalışmak, ekonomik ve toplumsal yaşamımızı önemli ölçüde kısıtlar altına sokacaktır. Bugünden öngörülemez ölçüde zararlar verebilir. Ülkemizde bilgi teknolojilerinin üretimini, tüketimini ve içeriğini zenginleştirmek üzere yapılanmalara gitmek, elektronik belge ve sayısal imzalar gibi gerekli öncül yasaların çıkarılmasını sağlamak çok daha acil sorunlar olarak karşımıza çıkmaktadır. Bu bağlamda, bilgi güvenliğinin sivil uygulamalarını kapsam dışında tutmalıdır.

1. Bkz. The National Security Agency, http://www.nsa.gov/about_nsa/faqs_internet.html.
2. Bkz. The National Security Agency,
http://www.nsa.gov/about_nsa/faqs_internet.html
3. Bkz. The National Security Agency
http://www.nsa.gov/about_nsa/faqs_internet.html
4. Bkz. Key to Secret Drawers: The Clipper Chip and Key Escrow Encryption
<http://www.stardot.com/~lukeseem/j202/essay.html>
An Introduction Cryptography–PGP Documentation, <http://www.pgp.net>
E–Commerce and the Encryption Debate, Stuart J. D. Schwarzstein, Institute for Prospective Technological Studies
Report No. 42 – JRC – Seville March 2000.
5. Bkz. White Paper: "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision
Directive 63"
<http://www.whitehouse.gov/WH/EOP/NSC/html/documents/NSCDoc3.html>
6. Bkz. Government Communications Headquarters, <http://www.gchq.gov.uk/>
7. Bkz. Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.de/>
8. Bkz. EPIC Electronic Privacy Information Center, An International survey of Encryption
Policy, 1999, sayfa 80.
OECD DSTI/ICCP/ REG(98)4/FINAL, "Inventory of Controls on Cryptography
Technologies", 1999, sayfa 28.
9. Bkz OECD DSTI/ICCP/ REG(99)13/FINAL, "Inventory of Approaches to Authenticatio
and Certification in a global Networked Society", sayfa 62. 10. Bkz. A Briefing on Public Policy Issues Affecting Civil
Liberties Online from the Center for Democracy and Technology, http://www.cdt.org/publications/pp_6.02.shtml
Preserving America's Privacy and Security in the Next Century: A Strategy for America
in Cyberspace, <http://www.cdt.org/crypto/CESA/CESAwhitepaper.shtml>
11. Bkz. Address by Prime Minister Lionel Jospin at the 20th Summer Forum on Communication,
<http://www.internet.gouv.fr/english/textesref/hourtin99.htm>
France in the Information Society, <http://www.internet.gouv.fr/english/textesref/letter.htm>
Preparing France's Entry into the Information Society
<http://www.internet.gouv.fr/anglais/sommaire.htm>
12. Bkz. OECD DSTI/ICCP/ REG(98)4/FINAL, "Inventory of Controls on Cryptography Technologies", 1999, sayfa 28.
13. Bkz. E–Commerce and the Encryption Debate, Stuart J. D. Schwarzstein, Institute for Prospective Technological
Studies Report No. 42 – JRC – Seville March 2000.

Kaynakça

1. The National Security Agency (http://www.nsa.gov/about_nsa/faqs_internet.html).
2. Keys to Secret Drawers: The Clipper Chip and Encryption

(<http://www.stardot.com/~lukeseem/j202/essay.html>).

3. *An Introduction Cryptography–PGP Documentation.*

4. *The IPTS Report, E–Commerce and the Encryption Debate by Stuart J. D. Schwarzstein, IPTS No. 42 – JRC – Seville March 2000*

5. *WHITE PAPER The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 May 1998. This White Paper,*

(<http://www.whitehouse.gov/WH/EOP/NSC/html/documents/NSCDoc3.html>)

6. *Government Communications Headquarters, (<http://www.gchq.gov.uk/>).*

7. *Bundesamt für Sicherheit in der Informationstechnik,*

(<http://www.bsi.de/>).

8. *EPIC, An International survey of Encryption Policy, 1999,*

9. *OECD, Inventory of Controls on Cryptography Technologies, 1999,*

DSTI/ICCP/REG(98)4/FINAL

10. *OECD; Inventory of Approaches To Authentication And Certification In a Global Networked Society, 1999,*

DSTI/ICCP/REG(99)13/FINAL

11. *CDT POLICY POST Volume 6, Number 2 January 21, 2000,A Briefing On Public Policy Issues Affecting Civil Liberties Online From The Center For Democracy And Technology*

(http://www.cdt.org/publications/pp_6.02.shtml)

12. *Preserving America's Privacy And Security In The Next Century.,A Strategy For America In Cyberspace, A Report To The President Of The United States*

<http://www.cdt.org/crypto/CESA/CESAwhitepaper.shtml>

13. *Address by Prime Minister Lionel Jospin at the 20th Summer Forum on Communication,*

<http://www.internet.gouv.fr/english/textesref/hourtin99.htm>

14. *France in the Information Society, <http://www.internet.gouv.fr/english/textesref/letter.htm>*

15. *Preparing France's entry into the inform@tion society, Government action programme, January 1998,*

<http://www.internet.gouv.fr/anglais/sommaire.htm>).

www.stradigma.com

aylık strateji ve analiz e–dergisi