TÜRKİYE BÜYÜK MİLLET MECLİSİ

YASAMA DÖNEMİ	YASAMA YILI
24	2

(10/108, 155, 156, 157, 158, 159, 160) ESAS NO'LU BİLGİ TOPLUMU OLMA YOLUNDA BİLİŞİM SEKTÖRÜNDEKİ GELİŞMELER İLE İNTERNET KULLANIMININ BAŞTA ÇOCUKLAR, GENÇLER VE AİLE YAPISI ÜZERİNDE OLMAK ÜZERE SOSYAL ETKİLERİNİN ARAŞTIRILMASI AMACIYLA KURULAN MECLİS ARAŞTIRMASI KOMİSYONU

TUTANAK DERGİSİ

09 Mayıs 2012 Çarşamba

(10/108, 155, 156, 157, 158, 159, 160) ESAS NO'LU BİLGİ TOPLUMU OLMA YOLUNDA BİLİŞİM SEKTÖRÜNDEKİ GELİŞMELER İLE İNTERNET KULLANIMININ BAŞTA ÇOCUKLAR, GENÇLER VE AİLE YAPISI ÜZERİNDE OLMAK ÜZERE SOSYAL ETKİLERİNİN ARAŞTIRILMASI AMACIYLA KURULAN MECLİS ARAŞTIRMASI KOMİSYONU

GÖRÜŞME TUTANAKLARI

09 Mayıs 2012 Çarşamba

----0----

K O N U

İ Ç İ N D E K İ L E R

Açılma Saati: 12.44
Kapanma Saati: 13.54

9 Mayıs 2012 Çarşamba

BİRİNCİ OTURUM

Açılma Saati: 12.44

BAŞKAN: Necdet ÜNÜVAR (Adana)

BAŞKAN VEKİLİ: Yıldırım M. RAMAZANOĞLU (Kahramanmaraş)

SÖZCÜ: İlhan YERLİKAYA (Konya)

KÂTİP: Erdal AKSÜNGER (İzmir)

----- 0 -----

BAŞKAN – Bilişim ve İnternet Komisyonumuzun çok değerli üyeleri değerli milletvekillerimiz, değerli konuklarımız, değerli uzmanlar ve basın mensupları; hepinizi saygıyla selamlıyorum.

Bugün sabah, medya mensuplarıyla bir kahvaltımız vardı. Oradan çıktık ve koşa koşa buraya geldik. Güzel, verimli bir toplantı oldu.

Şimdi bugün Bilgi Güvenliği Derneği temsilcilerini dinleyeceğiz. İnternet'te hep karşımıza çıkan bir husustur bilgi güvenliği. Bununla ilgili, inşallah, oldukça verimli bir toplantı yapacağımızı umuyorum ve şimdi, Bilgi Güvenliği Derneği Yönetim Kurulu Başkanı, aynı zamanda Gazi Üniversitesi Teknoloji Fakültesinde Öğretim Üyesi Sayın Profesör Doktor Mustafa Alkan'a söz vereceğim.

Buyurun Değerli Hocam, söz sizde.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Teşekkür ediyorum.

Sayın Başkanım, sayın üyeler, sayın konuklar; öncelikle hepinizi saygıyla selamlıyorum. Bize bu fırsatı verdiğiniz için de teşekkür etmek istiyorum.

Ben arkadaşlarımı da tanıştırmak istiyorum: Yönetim Kurulundan Profesör Doktor Şeref Sağıroğlu, bizim Derneğimizin İkinci Başkanı; Hakan Yıldırım, yine Derneğimizin Yönetim Kurulu üyesi, aynı zamanda Türkiye Büyük Millet Meclisi Bilgi İşlem Başkan Yardımcısı; Ali Yazıcı Bey de ASELSAN'dan, Türkiye'deki millî kriptoları ve millî güvenlik tarafını yürüten grubun başındaki Bilgi Güvenliği Müdürü arkadaşımız.

BAŞKAN – Değerli Başkan, affedersiniz, sunuma başlamadan, sunumunuzun hardcopy'sini vermiş miydiniz?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Çok özet hâlinde kitapçık şeylerin içerisinde dağıttık. Özetini, sunum biraz uzun ama arzu edilirse hardcopy'sini de sizlerle paylaşırız Başkanım.

BAŞKAN – Tamam.

Buyurun efendim.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Sayın Başkanım, hızlıca özetlemeye çalışacağım, konu oldukça uzun ve yoğun bir konu. Hepinizin bildiği gibi, siber güvenlik, siber saldırılar, siber savaşlar konusu, bütün dünyayı çok yakından ilgilendiren bu konular tüm dünyada olduğu gibi son zamanlarda bizim ülkemizde de en önemli gündem maddelerinden biri hâline geldi.

Ben kısaca bir ön giriş olması açısından şunu söylemek istiyorum. Artık dünyada ülkelerin zenginlikleri iki şeyle ölçülüyor: Bir, ne kadar bilgi miktarına sahip olduklarıyla, ikincisi de ne kadar bilgili insana sahip olduklarıyla ölçülüyor. Dolayısıyla, her şey bilgi etrafında dönmeye başladı. Bu da iki şeyi getirdi: Teknoloji geliştikçe günümüzde bilgi miktarı artıyor, bilgi miktarı arttıkça da teknoloji gelişiyor. Pozitif bir geri beslemeyle, ülkelerin bilgi miktarının ya da teknolojik gelişmelerinin temelini sağlayan bilgi olduğu.

Hepimizin bildiği gibi, dünyada iki temel şey var artık; Bir, dünya bilgi toplumuna dönüşme sürecinde ve tüm ülkeler de bu değişim sürecine ayak uydurabilmek ve bu süreci gerçekleştirmek için yoğun bir çaba sarf ediyor. Biz de ülke olarak bu yönde iki temel değişimi gerçekleştirmeye çalışıyoruz. Bilgi toplumu olmanın birinci temel şartı, fiziksel değişim, ikinci temel şartı da kültürel değişim. "Fiziksel değişim" dediğimiz şey, ülkenin bilgi ve iletişim teknoloji altyapılarına en iyi şekilde sahip olabilmek ve bu teknolojileri en iyi şekilde kullanma kültürüne sahip olabilmek. Ülke olarak teknolojilere sahip olma noktasında çok önemli noktaya geldiğimizi söyleyebiliriz; uluslararası ortalamaların da üzerinde bilgi teknolojileri, donanımlar, İnternet, bilgisayar sahiplik oranı, İnternet sahiplik oranı, geniş bant sahiplik oranı gibi altyapılarda önemli bir değişim oldu ancak kültürel değişim noktasında biraz sıkıntılarımız var, onu biraz sonra sizlerle paylaşmak istiyorum.

Her şey bilgi etrafında dönmeye başlayınca bilginin ne olduğunu kısaca özetlemek gerekirse, "bilgi" dediğimiz şey, bir devlete ait askerî, mali, enerji ve benzeri bilgileri, bir şirkete ait altyapı, yatırım, borç, alacak bilgileri, bir üniversiteye ait ya da teknoloji merkezlerine ait ar-ge bilgileri, kişilere ait özel iletişim ya da özel bilgiler, üst düzey kişilere ait sağlık bilgileri gibi tüm bu bilgiler bizim için önemli bilgiler. Eğer bu bilgiler rakiplerin ya da düşmanların eline geçmesi hâlinde de büyük zararlar vereceği ve dolayısıyla bu bilgilerin korunmasının gerektiği de günümüzde son derece önem arz ediyor ve ortaya bir kavram çıkıyor. Bu bilişim ortamında, her şeyin elektronik ortamına dönüştüğü ve sanal ortamda bilgiye dönüştüğü bir durumda ve hepimizin de hemen hemen bu sanal ortamı, İnternet ortamını, bilişim ortamını kullandığımız durumda yeni bir kavram ortaya çıkıyor, o da "e-Birey" kavramı. Eğer toplumlar bu "e-Birey" kavramını sağlıklı bir şekilde oluşturamazlarsa, bilgi ve iletişim teknolojilerini kullananlar e-Birey olmanın gereklerini ve şartlarını yerine getiremezlerse çok ciddi problemlerin doğacağı ve örneklerle de, dünyada yaşandığı gibi yaşanacağı hepimizin malumu.

Öyleyse birinci şart, ülkelerin en önce yapmaları gereken, e-Birey'lerini oluşturması gerekiyor. İlkokuldan üniversiteye ve toplumun tüm kesimlerinde en üst görevden en aşağısına kadar kişilerin bir e-Birey olması ve e-Birey'in niteliklerini ve özelliklerini kazanması gerekiyor. Eğer toplumda bilgi ve iletişim teknolojilerini kullanan kişiler bu e-Birey olmanın gereklerini yerine getiremezse bugün günümüzde yaşamış olduğumuz siber saldırılar, sanal saldırılar karşısında ne yazık ki kendimizi koruyabilmemiz, bilgi ve değerli varlıklarımızı, kıymetli varlıklarımızı -biraz sonra bahsedeceğim- koruma imkânına sahip değiliz. İşte, bu "kültürel dönüşüm" dediğimiz şey, toplumdaki bireylerin e-Birey hâline gelebilmesi.

Nedir e-Birey hâline gelebilmesi? Bir defa, artık bu çağda herkesin bir bilgi profesyoneli olması gerekiyor; ikincisi, yeterli bilgi kaynaklarına sahip olması gerekiyor; üçüncüsü, yeni düşünceler, yeni yaklaşımlar oluşturabilmesi gerekiyor, sanal etki gruplarında tanınabilmesi ve bireysel küreselleşmeyi

sağlaması gerekiyor. Sonuçta, tüm dünyadaki bu entegrasyonu, küreselleşmeyi artık bireysel anlamda bilişim ortamında, İnternet ortamında sağlıyoruz.

Bir de herkesin, bulunduğu pozisyonda ve görevde amaçlarına uygun rol üstlenebilmesi ve rol dağılımı yapabilmesi gerekiyor.

Sonuçta ortaya şöyle bir durum çıkıyor: Hepimizin "siber dünya" diye tanımladığımız, "sanal dünya" diye de tanımladığımız dünyada artık hayatın her yönüyle sayısallaştığını görüyoruz. Hayatımızın her evresinde bütün iş ve işlemlerimizin sayısallaştığını ve uluslararası protokollerin ve standartların da hayatın tüm evrelerine nüfuz ettiğini görüyoruz. Buna da bütün dünya "siber dünya" diyor.

İşte bu siber dünyada, baktığımız zaman, çok yoğun bir şekilde bir bilgi miktarı dolaşıyor. 1,6 milyar İnternet kullanıcısı var, günde 247 milyar e-Posta dolaşıyor. Artık tüm iş ve işlemlerimizi de elektronik ortamda yapıyoruz. Yani 240 milyon İnternet adresi, 20 milyara yakın İnternet sayfası, 2 milyar civarında resim, 50 milyon ses, görüntü dosyası bu sanal ortamda dolaşıyor. Bu şu demektir: Artık bizim bütün bilgilerimiz, iş ve işlemlerimiz sanal ortama, elektronik ortama akmış durumda.

2011 OECD ülkelerine baktığımızda da yetişkin kullanıcılar da dâhil olmak üzere, kamu kurum ve kuruluşlarındaki, sektördeki, özel hayatımızdaki işlemlerimizin de büyük çoğunluğunun bu sanal ortamda gerçekleştiğini görüyoruz ve yeni birtakım eğilimler doğuyor bu süreçte. İnternet faaliyetleri var, bir de sosyal medya var. Sosyal medya tarafına, sanıyorum daha önceki sunumlarda girildiği için çok girmek istemiyorum ama İnternet faaliyetlerine baktığımız zaman, biraz önce söylediğim gibi, hayatımızdaki tüm iş ve işlemlerimizin bu ortamda gerçekleştiğini görüyoruz ve bu süreç öyle hızlı ilerliyor ki 2006'da 12 milyon olan Facebook kullanıcısı 2012'de 1 milyara kadar ulaşıyor. Burada şunu göstermeye çalışıyorum: Artık süreç öyle bir hızlı ilerliyor ki bu sanal dünya, sanal ortam hayatımızın her devresine nüfuz ediyor.

Küçük bir örnek olması açısından söylemek istiyorum: Eylül 1971'de İnternet bağlantısı bu şekildeydi yani iki tane hat vardı bir bölgeden bir bölgeye. Sadece bu iki hat üzerinden İnternet haberleşmesi gerçekleşirken bugün geldiğimiz noktada İnternet ağı böyle.

Bu şu demektir: Dünyada artık her şey İnternet üzerinden gerçekleşiyor ve bu siber dünyada, sanal dünyada böyle bir iletişim ortamı, iletişim dünyası var. Şimdi bu dünyanın güvenliği son derece önem arz etmeye başlıyor çünkü tüm ülkelerin, tüm milletlerin her türlü ilişkileri bu ortamda gelişiyor. Dolayısıyla, dünya yeni bir kavramla yüz yüze gelmeye başladı. Siber savaşlar ve siber güvenlik konusu.

"Siber savaş" dediğimiz olay şu: Kişilere, şirketlere, kurumlara, örgütlere, bilgi sistemlerine veya iletişim altyapılarına yapılan planlı, koordineli saldırılara -ticari, politik veya askerî amaçlı olabilir- "siber saldırı" diyoruz. Nitekim bunları günümüzde 7/24 saat yaşıyoruz. Bir kısmının farkındayız, bir kısmının farkında değiliz ama tüm dünyada olduğu gibi, en yoğun saldırıya uğrayan ülkeler arasındayız biz bu konuda. Dünya sıralamasına baktığımız zaman neredeyse ilk üçlerde, ilk onlarda sürekli geziyoruz; böyle yoğun bir saldırı var.

Bir de siber savaş var. Aynı saldırılar ülke veya ülkelere yönelik yapılıyorsa buna da "siber savaşlar" diyoruz. Örnek vermek gerekirse hepimiz gördük; Anonymous, Türkiye'ye, bazı kurumlara yönelik saldırılar yaptı, dedi ki: "Ben şu kurumlara, şu gün, şu saatte saldıracağım." Bunlara "siber saldırı" diyoruz ama yine

hepimizin bildiği Wikileaks olayına da "siber savaş" diyoruz. Wikileaks gerçekten resmen bir siber savaştır, bütün dünya çapında gerçekleşmiş bir olaydır. Anonymous'un bizim ülkemizde yoğun bir şekilde ve başka ülkelerde de yaptığına da "siber saldırılar" diyoruz ve bunları sürekli yaşıyoruz. Bir kısmının farkındayız, bir kısmının farkında değiliz. Bir kısmını açık ediyorlar, söylüyorlar "Şuralara saldıracağız." diye ama bir kısmından hiç kimsenin, hiç birimizin, kurum, kuruluşlar dâhil, ülkeler de dâhil, en kritik kurumlarımız da dâhil ne yazık ki bazılarının farkında olmuyoruz.

Dolayısıyla, ortaya "siber güvenlik" kavramı geliyor. Bizim bütün bu saldırılar karşısında siber güvenliğimizi nasıl sağlayacağımızı, nasıl oluşturacağımızı bilmemiz gerekiyor. İşin ciddiyetini vurgulama adına, yine hepimizin basından, medyadan duyduğumuz, bildiğimiz olay, ABD Başkanı Obama'nın gelir gelmez ilk yaptığı iş, siber güvenlik konusuna el atmak oldu ve şöyle bir deklarasyon yayınladı. Dedi ki: "Ülke olarak karşılaşılan çok ciddi, ekonomik ve ulusal güvenlik sağlama hedeflerinden birisi olup Hükûmet veya ülke olarak henüz tam anlamıyla önlem alamadığımız bir hususdur."

Her türlü saldırılara karşı, askerî saldırılara karşı, başka türlü saldırılara karşı önlem alabiliyorlar bu teknolojinin en hâkim konumundaki ülke olan ABD ama diyor ki: "Siber saldırılara karşı önlem alamadığımız bir durum bu." Bunun için bir anlamda alarm veriyor ve çok ciddi çalışmalar ve faaliyetler gerçekleştiriyor.

Aynı şekilde örnek olsun diye bunu paylaşıyorum. Beyaz Saray Siber Güvenlik Sorumlusu bu işin başındaki uzmanlardan biri olan Richard Clarke şöyle bir örnek veriyor, diyor ki: "Artık biz Sinop'taki kuleyi kullanmıyoruz. Biz Sinop'taki kulemizden Rusya'nın bütün haberleşmesini izliyorduk ama artık Rusya'daki konuşmaları, haberleşmeleri izlemek için ya da istihbarat işlemlerimizi gerçekleştirebilmek için böyle kulelere gerek yok çünkü artık Amerika'da oturarak, dünyanın bir yerinde oturarak casuslar ülkelerin bütün bilgilerine erişebiliyorlar, ulaşabiliyorlar ve ne konuşuyorlar, ne yazışıyorlar, ne yapıyorlar bunlardan haber alıyoruz."

Burada şunu söylemeye çalışıyorum: Artık istihbaratın da işte ajanlığın da ajanların da şekil değişti, tarzı değişti, uygulaması değişti. Bu sanal dünyada yepyeni bir istihbaratçılık süreci başladı ki ülkeler de bunun gereğini yapıyorlar.

Önce şunu söyleyeyim: Ülkeler bu işin vahametinin ve ciddiyetinin farkında olduğu için çok ciddi yatırımlar yapmaya başladılar. Ta, 2002 yılında ABD, sadece siber güvenlik konusuna, siber savunma konusuna 2,7 milyar, 2003 yılında ise 4,2 milyar yatırdı. Bugün 12 milyon dolar günlük harcama yapıyor ABD; günde 12 milyon dolar harcaması var sadece siber savunma üzerine ve ciddi anlamda da siber ordularını oluşturabilmek için -yine hepimiz biliyoruz- siber ordusunu kurdu. Biraz sonra bahsedeceğim, sadece ABD değil diğer ülkeler de dâhil olmak üzere ABD, Rusya, Çin, İsrail ve İngiltere gibi ülkeler tamamen savunma ve saldırı timleri oluşturdular günümüzde. Bu ülkelerin hepsinde siber ordular var, bunları hem savunma amaçlı kullanıyorlar hem de saldırı amaçlı kullanıyorlar. Sadece bunlarla da yetinmiyorlar, taşeron hacker'ler kullanıyorlar ülkeler çünkü uluslararası suçlara karışmamak için ya da devlet olarak yapamayacağı işler için, taşeron hacker'ler ya da taşeron organizasyonlar tarafından bu işleri gerçekleştiriyorlar. Bunlarla ilgili de yoğun çalışmalar olduğunu görüyoruz.

Dolayısıyla, artık teknolojinin ulaştığı noktada doğrudan bir silah olarak bu teknolojilerin kullanılabildiğini görüyoruz. Yani klasik savaş teknolojileri ya da teknikleri artık günümüzde kullanılmıyor, bu

teknolojiler kullanılıyor. Nitekim yine CIA Başkanı "Soğuk savaş bitti ama teknoloji savaşları başladı." diyor. Yine ABD eski Savunma Bakanı Albright'da "Siber saldırılar NATO'ya karşı üç tehditten biri kabul edilecektir." diye, biliyorsunuz deklarasyon yayınladı ve artık siber saldırılar resmen dünyada savaş sebebi hâline geldi.

Ne tür işlemler yapılıyor bu siber savaşlarda? Casusluk işlemleri yapılıyor, ülkelerin istihbaratlarıyla ilgili tüm işlemler gerçekleştiriliyor, manipülasyonlar yapılıyor, propaganda yapılıyor buralar üzerinde, iletişim gerçekleştiriliyor ya da iletişim altyapıları tamamen çökertiliyor, virüsler bulaştırılıyor -biraz örnekleri de vereceğim- "Truva atları" dediğimiz, tüm sistemler bozulabiliyor, siber bombalarla sabotajlar yapılabiliyor, bilgi kirliliği oluşturuluyor, sistemler kilitlendiriliyor, dolandırıcılık, banka soygunculukları, ekonomik şeyler gibi birçok işlemler gerçekleştiriliyor.

Örnek vermek gerekirse, nitekim hepimizin çok yakından bildiği iki temel örnek var; dünyada ilk "siber savaş" diye tarihe geçen, biliyorsunuz 2007'de Estonya siber savaşı, 2008'de Gürcistan siber savaşı. Her ne kadar bağımsız gibi görünse de hâlâ Rus peyki olan bu iki ülke Rusya için mükemmel bir deneme oldu. Malum, biliyorsunuz, bir meydandaki heykeli kaldırmaya kalkınca Estonya, Rusya bu ülkelere karşı siber saldırı gerçekleştirdi ve Estonya'nın da, Gürcistan'ın da yaklaşık bir ay boyunca bütün finans, basın-yayın, iletişim, kamu işlemlerinin altyapıları tamamen işlemez hâle geldi, devlet kitlendi kaldı, bir ay hiçbir işlem yapamadılar. Biraz sonra ne tür şeyler olacağını daha somut örneklerle vermek istiyorum. Dolayısıyla NATO bu iki ülkeyi savunabilmek için 2008 yılında Estonya'da Siber Savunma Merkezi kurdu çünkü artık, hem Estonya hem de Gürcistan'ın devlet iş ve işlemleri, altyapıları tamamen çöktüğü için hiçbir şey yapamaz hâle gelmişlerdi. Bunun üzerine ABD Savunma Bakanı ülkelerin füze sistemlerini, enerji boru hatlarına, basın-yayın merkezlerine yapılan siber saldırıları savaş sebebi saydı çünkü bu saldırılar çok yoğun bir şekilde gerçekleşiyordu ve klasik savaş unsurlarıyla da karşılık vereceğini söyledi çünkü aynı saldırılar ABD'ye karşı da yoğun bir şekilde yapılıyordu. Rusya'nın bu saldırısı karşısında, virüslü bir hafıza kartıyla yine aynı şekilde ABD'nin Irak ve Afganistan savaşlarını yürüten komuta merkezine sızdı ve ciddi sonuçlar aldı. Şunu yaptılar: Afganistan'da rastgele satılan bizim bildiğimiz bu flash bellekleri dağıttılar, onların içerisine casus yazılımlar, virüsler yerleştirdiler. Oradan biliyorsunuz Rus askerleri ya da komutanları o flash bellekleri Afganistan'dan satın alıp kendi komuta merkezlerine gittiklerinde o flash bellekler bütün Afganistan'daki ABD'nin komuta merkezlerindeki bilgilerin tamamını aktardı. Bu şekilde basit uygulamalar bile ciddi sonuçlar doğurdu. ABD daha sonra bundan haberdar oldu ve şu açıklamayı yaptı: "Sızıntının nerelere kadar ulaştığını bilmiyoruz." Bunun böyle de bir tehlikesi var. Yine ABD kongresine yapılan bir sunumda, Çin'in sadece Tayvan'a bir müdahale gerçekleştirmek için ABD'nin harekete geçmesini engelleyecek yeterli düzeyde siber silahtan yararlanabilecek konumda olduğu açıklandı çünkü en önemli şeylerden bir tanesi de, güçlü silahlarından bir tanesi de dünyada yine Çin'in siber gücü. Rusya'nın saldırısına karşı ABD İran'a bir saldırı yaptı, yine medyadan gördük; "stuxnet" diye bir yazılımla İran'ın bütün nükleer sistemlerini çökertti. Oraya göndermiş olduğu bu yazılımla, virüsle santrifüjleri kontrol altına aldı ve nükleer santrallerdeki santrifüjler delice dönmeye başladı ve tamamen İran'ın nükleer santralleri çalışmaz hâle geldi, iflas etti ve İran Devlet Başkanı da açıkça bunu deklare etti. Bundan sonra tabii ki 62.867 tane bilgisayarını çökertti İran'ın, sadece bir virüs. İran bilgi

işlem altyapısı neredeyse çöktü bu virüsle birlikte. Ama İran hazırlıklı olan bir ülkedir ve bu konuda en iyi siber savunmasını, ordusunu geliştirmiş ülkelerden bir tanesidir. Hemen karşılık verdi. İran'ın bu virüsteki kodlarını çözüp antivirüs kodlarla Amerika'nın bütün sistemlerini geriye döndürerek neredeyse durduracak hâle getirdi, İran tehdidine karşı da Amerika siber savunma alarmı verdi. Biraz sonra örnekler vermek istiyorum, burada birçok açıklamaları var bu saldırıların nerelere geldiğiyle ilgili ve ABD'yi durduran İran silahları bu siber savunma silahları oldu. Mesela, İran, siber silahlarıyla şunları yapabiliyor şimdi: ABD'nin hayalet uçakları teknolojisindeki şifreleri kırarak uçakları sistem dışı bırakabiliyor. Aynı şekilde insansız uçakların iletişim ve füze hedefleri teknolojilerini kırarak onları çalışmaz hâle getirebildi. "Elektromanyetik darbe barajı" veya "füze saldırıları" dediğimiz ABD ve İsrail askerî üslerini haritadan sildi yani bütün konum, pozisyon bilgilerini çalışmaz hâle getirdi. Aynı zamanda da modern bir Truva atı donanması oluşturdu. "Uyuyan süper virüs kıyamet günü siber saldırılarının ilk dalgasında tetiklenir." diye şurada anlatmaya çalıştığım şeylerle ABD'nin bütün teknolojik şeylerini neredeyse durdurur, işletmez ve bir karşı güç hâline getirebildi İran bu siber savunma gücüyle beraber.

Burada şunları anlatmaya çalışıyorum: Şimdi, artık, günümüzde hakikaten tüm dünya, savaşlarını böyle yapıyor ve bizim kritik altyapılar var. Biz hep şunlara yoğunlaşıyoruz: İşte "Falanca kurumun sayfası hacklendi, falanca yere girildi, falanca bilgiler deşifre edildi." falan filan. Bunlar işin hakikaten çok basit tarafı, önemsiz tarafı, çok tehdit ve tehlike oluşturmayan tarafı ama siber savaşlarla, teknolojilerle, artık, "kritik altyapılar" dediğimiz altyapılarla ilgili büyük tehdit ve tehlikeler başlıyor. Nedir o? Bütün trafik ışıklarını kontrol ederek tüm trafiği altüst edebiliyorlar, hava trafiğini kontrol ederek uçakları havadan indirmez kaldırmaz hâle getirebiliyorlar, enerji nakil hatlarını tamamen yok edebiliyorlar, doğal gaz boru hatlarını. Çünkü bunların tamamı -biraz sonra göreceğimiz gibi- bu altyapılar, hepsi sonuç itibarıyla bilgi işlem sistemleriyle yönetiyor. Bütün dünya şunu kabul ediyor: Kritik altyapılar; enerji, su, gıda, finans, sağlık, vesaire gibi şeyler. Bu, şu demektir: Bizim enerji sistemlerimizdeki, enerji nakil hatlarımızdaki gerilimi yükseltmesi ya da azaltması, 220 voltu 240-250 volta çıkarması demek bütün sistemlerin, bütün elektrikli aletlerimizin off olması yani sistem dışı olması, çalışmaz hâle gelmesi demek. Doğal gaz boru hatlarındaki basıncı artırması, tüm doğal gaz boru hatlarının patlaması, yangın çıkması…Yahut da en basitinde şunu yapabiliyorlar: Su depolarındaki klor miktarı bilgisayar sistemleriyle ayarlanıyor yani "Şu kadar litre suya şu kadar klor atılacak." O klor miktarını artırıyor ve farkında olmadan toplumun önemli bir miktarını klor zehirlemesi yapabiliyorlar. Aynı şekilde başka türlü işlemler de gerçekleştirebiliyorlar. Dolayısıyla bu kritik altyapıların tamamı günümüzde bilişim sistemleriyle yönetiliyor ve bu da ciddi bir savaş sebebi hâline getirilebiliyor. Örnek olsun diye söylüyorum: ABD'nin SCADA sistemi burası ve ABD bunu savunamaz hâle geliyor bu kadar güvenlik olmasına rağmen. ABD hava trafik kontrol sistemi… Bunların hepsi uçakla. Eğer bu sistem birilerinin eline geçirildiğinde -biraz sonra söyleyeceğim- "köle bilgisayarlar" dediğimiz… Nitekim sistemler köleleştiriliyor, bizim ülkemizde de var -2010 yılındaki rakamlar- bizim ülkemizdeki serverların 2 bin tanesi köle serverdır. Geliyorlar, bu hava kontrol sisteminin serverını, bilgisayarlarını ele geçiriyorlar dünyanın bir ucundan, orayı nasıl isterse öyle yönetiyorlar. Yönetince en az yüzlerce uçak birbirine çarpacaktır, düşecektir ya da hava trafiği tamamen kitlenir hâle gelecektir. Sistem bu kadar önemli hâle gelebiliyor. Aynı şekilde biraz önce dediğim gibi,

enerji, ulaşım, doğal gaz ve iletişim altyapıları… Biz diyoruz ki işte "Şunlar oldu, bunlar oldu; şu sebepten oldu, bu sebepten oldu." ama arka planda neler olduğunu ne yazık ki bilmiyoruz. Dolayısıyla böyle kritik altyapılara karşı ciddi tehdit ve tehlikeler var ve yakın gelecekte ülkelerin savaşları da bu şekilde olacak ve bu yönde olacaktır dolayısıyla ciddi anlamda bir siber tehditle, siber savaşla bütün dünya ülkeleri olduğu gibi bizim ülkemiz de karşı karşıya. Bu durumda ülkelerin savunmalarını nasıl geliştirdiği ve neler yaptığı son derece önem arz ediyor.

Tehdit araçları var. Her geçen günde çok hızlı bir şekilde bu tehdit araçları gelişiyor, sayıları gün geçtikçe artıyor ve bu tehditleri yapan, saldıracak uzmanların sayısı da artıyor teknolojik gelişmeye paralel olarak dolayısıyla tehdit her geçen gün daha büyüyor. Yani saldırı araçları, saldırıyı yapacak uzmanların yoğunlaşması yoğun bir şekilde tehlike boyutlarını önemli noktalara getiriyor ve nitekim biraz önce söylediğim gibi bunun ekonomik boyutları da var tabii ki. Mesela, sadece bir tane virüsle Britanya'da geçen yıl siber saldırıların ülke ekonomisine maliyeti 20 milyar pounddu. Yılda 100 binden fazla siber saldırının yaşandığı ABD'de ise rakam tahminî olarak 100 milyar dolar civarında. Yani ABD'nin siber saldırıdan dolayı yılda harcadığı, kaybettiği rakam 100 milyar dolar. Bir tane virüs, "I Love You" virüsü yayıldı, hepimiz duyduk, 10 milyar dolar; "Nimda" virüsü 3 milyar dolar. Bu gibi virüsler ülkelere milyar dolarlık zararlar veriyor ama bunlar tabii ki çok görünen, bilinen şeyler değil. Dünya işte bu tehdit ve tehlike karşısında "5. Güç" dediğimiz siber ordularını kurmaya başladı. Bizim bildiğimiz kara, deniz, hava, uzay ve benzeri siber orduların yanında tüm dünya ülkeleri "5. Güç" dediğimiz siber ordusunu kurdu. İşte Başkan Obama da Sanal Orduyu kurup bu işin komutanlığına Microsoft'un eski şefini getirdiği gibi, başına da General Keith Alexander'ı getirip onun komutasında ordular kurdu ve şu anda dünyanın en güçlü ordusu hâlinde ABD dünyayla baş etmeye çalışıyor. Bununla ilgili örnekler var, bu işin ne kadar ciddi olduğuyla ilgili.

Aynı şekilde, Çin, dünyanın en büyük siber ordusuna sahip durumda. Rusya, Kuzey Kore, İsrail ve İran geliyor dünyadaki siber ordulara sahiplik konusunda. Tüm ülkeler bunlarla ilgili politika ve stratejiler geliştiriyor. Mesela, Çin, 2050 yılına kadar bütün bu hazırlıkları yapacağını söyledi. İngiltere 10 bin tane katılımcıya eğitim veriyor yani 10 bin kişilik siber ordu kurmaya çalışıyor. Geçen yıllarda -yine hepimiz biliyoruz- Japonya 5 bin kişilik siber polis ordusu kurdu. Böyle binlerde, 5 binlerde, 10 binlerde ülkeler ordular kuruyorlar.

Şimdi bizim ülkemizde hepimiz yaşıyoruz bunu. Wikileaks ya da Anonymous diyor ki: "Falanca kuruma saldıracağım." Biz de ise sadece o kurum ben ne yapacağım diye telaşa düşüyor, elinde ne kadar uzman varsa onlarla savunma yapmaya çalışıyor. Ama böyle savunma yapmamız, bu saldırılara böyle karşılık vermemiz, kendimizi korumamız kurumların kendi başlarına yapabileceği ya da mevcut elindeki uzmanlarla yapabileceği bir şey değil çünkü bu müthiş bir uzmanlık gerektiren bir şeydir. B

undan dolayı tüm ülkeler bir şey yaptılar yıllardan beridir: Siber güvenlik strateji belgeleri hazırladılar. Bizim de ülke olarak bugün özellikle üzerinde durmak istediğimiz şeylerden bir tanesi budur. Bizim Bilgi Güvenliği Derneği ile Ulaştırma Bakanlığıyla birlikte uzun süredir yaptığımız çalışmalardan bir tanesi budur ama henüz sonuçlandıramadık: Türkiye'nin de bir an önce siber güvenlik strateji belgesini hazırlayıp yayınlaması gerekiyor çünkü ABD yayınladı -ayrıntılarına girmek istemiyorum, bunları sizlerle

paylaşacağız- Hindistan yayınladı, Almanya yayınladı, Hollanda yayınladı, aklımıza gelebilen bütün ülkeler siber güvenlik strateji belgesi yayınladı. Bu, şu demektir: Bütün devletin kurum ve kuruluşları kendilerini savunabilmek için, bilgi kaynaklarını ve kritik altyapılarını koruyabilmek için nasıl bir strateji oluşturması lazım? Bunun için kurum, kuruluşlar ne yapması lazım? Bu strateji belgesini yayınlayıp tüm bunlarla ilgili gerekli hazırlıkları ve çalışmaları yapıp bitirmesi lazım. Tüm gelişmiş ülkelerin tamamında bu siber güvenlik strateji belgesi vardır. Devlet bu siber güvenlik strateji belgesi doğrultusunda altyapısını oluşturuyor, uygulamalarını ona göre şekillendiriyor.

Tehlikelerin boyutuna geldiğimiz zaman şöyle: Klasik savaşlarda topun menzili belli, füzenin menzili belli, silahların nereye kadar yapacağı belli, uçakların nereleri bombalayacağı, nerelere ulaşacağı, nereye kalkıp nereye ineceği belli ama siber savaşta bu savaşın menzili belli değil. Siz dünyanın bir ucunda oturuyorsunuz, dünyanın bir ucundaki ülkeyi çökertebiliyorsunuz, göçertebiliyorsunuz, her türlü zararı verebiliyorsunuz, her türlü bilgilerine erişip en mahrem devlet sırlarını elde edebiliyorsunuz. Dolayısıyla bu savaşın sınırı ve boyutu yok.

Birkaç örnek olsun diye söylemek istiyorum: Türkiye'ye yapılan saldırılara baktığımızda, 2001 yılından beri Türkiye yoğun saldırılar altında aslında. Birçoğunu biliyoruz, birçoğunu bilmiyoruz. En çarpıcı örnek olduğu için bu örneği almak istedim. Hepimiz biliyoruz, bu, dergiye de yansıdı, basına da yansıdığı için söyledik: Şimdi, diyelim ki bazı kurumlar, buradaki durumda bizim Millî İstihbarat Teşkilatımız mesela. Oranın güvenliği çok sağlam olduğu için oraya giremediler, şöyle bir yol denediler: Maaşını nereden alıyor? Halk Bankası ve Ziraat Bankasından alıyor kurum. Gittiler, Halk Bankası ve Ziraat Bankasının sistemlerine girdiler, oradan maaş alan, kurumun tüm çalışanlarını tespit ettiler. Dolayısıyla bizim kurumda almış olduğumuz güvenlik bir işe yaramadı, bizim elemanlarımızın tüm bilgileri ortaya çıkmış oldu. Bu gösteriyor ki öyle tek başına bir kurumun güvenliğini sağlama alması yetmiyor. Yani Meclis çalışanlarımızın güvenliğini şey altına alabiliriz ama Meclis "X" bankasıyla çalışıyor, bütün bilgilerimiz orada bizim, tüm bilgilerimiz o bankada. Meclis sağlam ama banka değil, oradan bütün Meclis çalışanlarının bilgilerine erişilebiliyor. Dolayısıyla savunma olayı, bu siber güvenlik olayı çok yönlü ve çok taraflı ele alınması gereken bir olay. Nitekim gördük, çok büyük badireler yaşamadan inşallah bu şeyi atlatırız diye düşünüyoruz. Cumhurbaşkanımızın sayfası çökertildi, Meclisimizin sayfası, Başbakanlığın, İçişlerinin, Dışişlerinin, Ulaştırma, Genelkurmay, MİT, Emniyet, BTK, TİB, yani çökmeyen, saldırılmayan ya da göçmeyen sitelerimiz kalmadı, bunlar hâlâ da devam ediyor. Nitekim geçenlerde de gördük, yine Emniyetimizin birtakım bilgilerinin sızdığını, başka yerlerin birtakım bilgilerinin sızdığını.

Bunlar aslında dediğim gibi işin belki çok önemsiz tarafları ama şöyle bir prestij tarafı var işin -ülkeler arasında da bu hakikaten bir güç gösterisi, prestij olayı hâline geldi- nitekim şunu yaptılar: "Tr" uzantılı tüm siteleri çökerttiler dünyada yani Türkiye anlamında "tr" uzantılı Google'ı, Microsoft'u, Yandex'i, Hotmail'i, Yahoo'yu. Bu sırf Türkiye'ye yapılmış bir saldırıdır. Sonuçta dediler ki: "Biz dünyada 'tr' uzantılı alan bırakmıyoruz." ve bütün "tr" uzantılı alanları çökerttiler. Bu, ülke için bir prestij meselesi ve tabii ki hoş olmayan bir durum, sonuçta bizim bu şekilde… Nitekim yine İçişleri Bakanımızın sayfasını göçertip…

REŞAT DOĞRU (Tokat) – Kim yaptı bunu?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Tabii ki bunları kimin yaptığı konusu çok tartışma getiren bir konu, bunun en kötü tarafı da bu; dünyanın neresinden geldiğini bilmiyoruz, kimin yaptığını bilmiyoruz, biraz önce söylediğim gibi sınırı belli değil. Aynı şekilde Millî Savunma Bakanımızın sitesi hacklendi, oraya hiç hoş olmayan sözler yazıldı; işte "Meclise de sıra geliyor, şu oluyor, bu oluyor." falan filan gibi şeyler. Yine BTK hacklendi, orada başka türlü şeyler yapıldı. MERNİS hacklendi, 70 milyon kişinin kimlik bilgileri İnternet'e dağıtıldı. İLSİS'te 687 bin öğretmene ait kayıtların tutulduğu İLSİS'in bilgileri aktarıldı; tuttu bir tanesi, öğretmenin bir tayinini Şırnak'a çıkardı kendi yapıyormuş gibi bu işlemi, mahkemelerle uğraştık. İşte UYAP'ta "Sinan Berberoğlu" diye; o, tespit edildi nasıl olduysa bir şekilde. Defalarca UYAP'a girdik; dosyalara, mahkeme kararlarına, şunlara, bunlara yaptık falan gibi şeyler oldu. Operatörlerdeki adres bilgileri, iletişim bilgileri paylaşıldı. Finans kurumları zaten Türkiye'de en çok saldırılara uğrayan hesapların boşaltıldığı bir durum; birçok kimselerin hesapları boşaltılıyor, hesaplar aktarılıyor. Dünyada bu zaten başlı başına uluslararası şebeke hâlinde yapılıyor, bu hesap boşaltmalar. Bankalar bu konuda son derece hakikaten mağdur durumdalar. Bu konuda tüm dünya ciddi sıkıntılar yaşıyor. Bunun gibi her gün devam eden saldırılar var. Dediğim gibi her geçen gün de bu tehdit artıyor.

Dahasını bir örnek olsun diye söylüyorum: Geçen 2010 yılında yaptığımız araştırmada 2 bin tane bilgisayarımız Türkiye'de köle idi yani dünyanın bir ucundan Amerika'da, Rusya'da, İsrail'de, Çin'de birileri bu bilgisayarları kontrol altına alıyor yani tutuyor, işte…

HAYDAR AKAR (Kocaeli) – Pardon, siz nasıl tespit ettiniz bu 2 bin serverın köle olduğunu?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Bunu uluslararası şeylere girdiğiniz zaman, zaman zaman tespit edebiliyorsunuz.

HAYDAR AKAR (Kocaeli) – Bunun tespit edilmesi demek herkesin bizim alanlarımızda cirit atıyor olması demek uluslararası kuruluşlar da dâhil olmak üzere.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Şöyle: Bu sadece Türkiye'ye has bir şey değil, bütün dünyanın tehlikesi böyle, bizde de böyle tabii ki.

HAYDAR AKAR (Kocaeli) – Tamam, kabul ediyorum da yani bunu tespit etmek demek, uluslararası bir firma veya başka bir kuruluşu tespit etmek demek onların da her tarafta cirit atıyor olması anlamına gelir.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – İşte zaten biraz önce verdiğim örnekler öyle yani İLSİS'in, MERNİS'in bilgileri bir şekilde gidiyorsa birileri o serverları… Bu sadece kurumların değil, kişilerinki de böyledir yani biri giriyor, sizin ofisinizdeki bilgisayarınızı kontrol altına alıyor; bu illa kurumlar olacak değil ya da "X" şirketinin bilgisayarlarını kontrol altına alabiliyor ve şöyle yapıyor: Mesela, spam yayan ülkeler sıralamasında Türkiye ilk 3'ün içerisindeydi ve sürekli uluslararası eleştiri alıyorduk. Bir öğrendik ki dışarıdan birileri bizim bilgisayarlar üzerinden spam yayıyor. Nitekim Türk Telekom, TTNET'le yapılan bir çalışmada 3'üncü sıradan 70'inci sıraya geriledik. Bu sonuçta hemen hemen bütün ülkelerin yoğun yaşadığı olay. İşte Wikileaks olayı; ABD'nin bütün bilgilerine girildi ve ne kadar bilgisi varsa bunlar alındı ve tüm dünyayla da paylaşıldı. Bu tüm dünyanın ciddi anlamdaki problemi, sadece Türkiye'nin problemi değil. Tabii ki burada biraz önce söyledim, "kültürel dönüşüm" dedim yani bilgisayar sahibi oluyoruz, İnternet sahibi oluyoruz ama kullanma kültürü noktasında problemimiz var.

Mesela, "Google" dediğimiz olay dünyada en çok tercih edilen arama motoru ama dünyanın en iyi casus yazılımı Google; bu sadece Türkiye için bir tehdit, tehlike değil, bütün dünya için böyle. Tüm dünya bu Google'ı kullanıyor ve arama motoru. Bu arama motorlarıyla bunun kontrolünde olan ülkeler dünyanın bütün bilgisini topluyor. Ülkelerin eğilimlerini, siyasi eğilimlerini, ticari eğilimlerini, sosyal eğilimlerini belirliyor, ona göre politikalar, stratejiler geliştiriyor. Kelime, cümle, resim, ses taraması yapabiliyor. Kim, nerede, ne zaman, ne yaptı, ne etti; bütün bunlarla ilgili arka planda istatistiki analizler yapıyor, veriler yapıyor. Dolayısıyla biz bunları yoğun bir şekilde kullanıyoruz. Mesela, bizim kurumlarımız... İşte Google'a baktığın zaman bu gizli yazılar Google'a düşebiliyor çünkü kurumlarımızın bu konuda da ciddi şekilde güvenlik olgusunu oluşturuyor, farkındalığını oluşturuyor olması lazım.

Dolayısıyla ortaya şöyle bir resim çıkıyor: Dünya bu tehdit ve tehlikeyle karşı karşıya. Bizim de üzerinde durmamız gereken tabii ki İnternet anlamında çocuklarımız ciddi risk altında, gençlerimiz ciddi risk altında. İnternet'in sosyal, psikolojik çok ciddi tehlikeleri var, zararları var içerik konusunda, İnternet içeriği konusunda ciddi zararlı içerikler var ama asıl tehdit ve tehlikenin büyük boyutu böyle.

Biz de Bilgi Güvenliği Derneği olarak zaman zaman BTK, TÜBİTAK, üniversiteler, kamu kurum ve kuruluşlarımız, bakanlıklarımızla beraber bu konuda bir farkındalık oluşturmaya çalışıyoruz. Bunun için uluslararası konferanslar, etkinlikler, sempozyumlar yapıyoruz. Nitekim tatbikatlar yapıldı; 2008'de bir tatbikat yapıldı, 2009'da yapıldı, 2010'da yapıldı. Uluslararası konferanslar gerçekleştiriyoruz ilgili tüm bileşenleri bir araya getirerek politikalar, stratejiler üretelim istiyoruz. Nitekim bu yıl 5'incisini gerçekleştireceğimiz uluslararası konferansın dokümanları sizlere dağıtmış olduğumuz dosyalar içerisinde var. Bu vesileyle hepinizi de davet etmek istiyoruz oraya. Burada yaptığımız da bu olaya, bu gerçeğe toplumumuzun tüm kesimlerinin farkındalığı noktasında, bilinci noktasında ve özellikle de kamu kurum ve kuruluşlarımızın, devletimizin de dikkatine çekebilmek ve bu konuda ciddi birtakım altyapılar oluşturabilmek istiyoruz. Sonuçta, bu tatbikatlarda finans, enerji, telekom, savunma, sağlık sektöründe ciddi çalışmalar gerçekleştirildi.

Tabii, durum biraz bu kadar karamsar ama ülke olarak biz ne durumdayız? Dünyada en iyi siber güvenlik uzmanlarına sahip ülkelerinden biriyiz insan kaynağı açısından. Ona "hacker" deniyor, "vesaire" deniyor ama biz öyle demiyoruz ve bu konuda bizim yaptığımız da çok şeyler var yani "biz" derken kendimizi kastetmiyoruz; Türkiye'de kendi başına, kendi çabalarıyla birtakım işler yapan uzmanlar var. Nitekim, 4 Temmuz 2003 yılında 11 askerimizin başına çuval geçirilmesinden sonra 1.500 Amerikan sitesi hacklendi, bunlar da önemli siteler, öyle rastgele siteler değildi. Ermeni yasa tasarısında yine yüzlerce site çökertildi. Bizim özellikle resmî kurumlarımızın sitelerine en çok Brezilyalı hackerlar saldırı yapıyorlardı; işte bizim Meclisimize, Cumhurbaşkanlığına, Başbakanlığa, şuralara, buralara en çok saldırılar Brezilyalı hackerlar tarafından geliniyordu. Bunun üzerine 10 binden fazla Brezilya sitesi hacklendi, bu saldırılar listesinde hacklenen ülkeler sıralamasında Brezilya 1'inci sıraya oturdu. Ondan sonra Brezilya, Türkiye'ye saldıramaz hâle geldi ve saldırmıyor da artık. Yani sonuç itibarıyla, bizim durumumuz öyle o anlattığım şeyler bir yana Türkiye olarak hafife alınacak, küçümsenecek bir durumda değil. Türkiye'de bu insan kaynağı, yetişmiş insan kaynağı... Nitekim, dediğim gibi, Türkiye'ye saldıran ülkeler ciddi ciddi de kaygı, endişe ve korku içerisinde, bunu da açık açık dünyadaki siber güvenlik uzmanları açıkça deklare ediyorlar. Aynı şekilde PKK ve bölücülük

propagandası yapan siteleri biliyorsunuz, çok yoğun bir şekilde propagandalar var. Buralarla ilgili şeyler var. Yine Fransa'da özellikle Kutlu Doğum Haftası marifetiyle özellikle Peygamber Efendimiz'e…

BAŞKAN – Bitiyor değil mi Hocam? Biraz hızlanırsak…

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Az kaldı, bitiyor.

…yapılan şeyler sonrasında 2.587 Avrupa sitesi hacklendi. Yine işte İslama karşı, Müslümanlığa karşı misyonerlik faaliyetleri ya da Kuzey Kıbrıs'la ilgili yapılan şeylerde birçok site çökertildi yani bizde bu siber savaşta karşı saldırılar, ataklar, vesaireler devam ediyor ama sonuç itibarıyla bizim temelde yapmamız gereken şeyler şunlar: Bir kere Türkiye'de ciddi bir yasal boşluğumuz var, bu yasal boşluğun giderilmesi lazım. İki: Bu konuda yetkili bir kurum yok Türkiye'de, siber güvenlik konusunda, siber savunma konusunda bir yetkili kuruma ihtiyacımız var. Bir an önce bir otoritenin Türkiye'de siber güvenlik konusunda ve savunma konusunda oluşması lazım. Ulusal bir strateji hazırlanması lazım, bir ulusal stratejimiz yok. Bununla ilgili bir düzenleyici çerçeve oluşturulması lazım yani bizlere bu tür saldırılar geldiğinde bizim ne yapmamız lazım, nasıl savunma yapmamız lazım ve Türkiye'nin bu tehdit, tehlikelerin karşısında nasıl hareket etmesi lazım? Bir başka madde: Farkındalık oluşturmamız lazım. Pervasızca İnternet kullanıyor herkes, pervasızca sosyal paylaşım sitelerinde dolaşıyoruz; Youtube'da, Facebook'ta her türlü bilgilerimiz aleni, açık ortalarda geziyor, kamu kurum ve kuruluşlarımız hakeza öyle. En yetkili kişilerimiz Hotmail kullanıyor, Yahoo kullanıyor, Gmail kullanıyor mail adreslerinde. Devletimizin önemli kurumlarında görev yapan yöneticilerimiz mail adreslerinde Gmail'i kullanıyor, Hotmail'i kullanıyor, Yahoo'yu kullanıyor; bu çok ciddi bir tehdit ve tehlikedir çünkü yapılan bütün yazışmalar, burada yapılan şeyler alenidir ve birilerinin eline geçme ihtimali son derece yüksektir. Devletin bu anlamda da birtakım politikalar üretmesi… Ve somut olarak da Türkiye'nin bir millî posta altyapısının da oluşturulması lazım yani Hotmail yerine, Gmail yerine, Yahoo yerine devlet kendi millî posta altyapısını oluşturup tüm kamu kurum ve kuruluşlarında kişilerin bu millî posta altyapısıyla çalışması lazım ki bununla ilgili projelerimiz de var, hazır hâle de getirdik, test uygulamalarını da gerçekleştirdik ama hayata geçiremedik bunları. Bunu dünya yaptı, birçok ülke; Çin'i, Almanya'sı, İngiltere'si, Fransa'sı, şunu, bunu. Hep millî altyapılarına geçtiler ama biz hâlâ Gmail'den, Hotmail'den, Yahoo'dan kurtulamadık. Burada örnekler var, siber güvenlikle ilgili neler yapacağımızın somut örnekleri var, bunları sizlerle paylaşacağız rapor hâlinde ve Türkiye'nin bir an önce bu adımları atarak siber savunma işlerini gerçekleştirmesi lazım. Son modelimiz de bu.

Türkiye'de bir an önce ulusal siber güvenlik otoritesini kurup kamu kurumları, kolluk kuvvetleri, vatandaşların emniyeti, maddi manevi olmayan değerlerin korunması, kritik altyapıların korunması, siber güvenliğin sağlanması, siber güvenliğin paydaşlarının, taraflarının belirlenmesi, bilgi toplama hizmetleri ve bir de siber savunma gücünün oluşturulması lazım bütün dünyanın yaptığı gibi. 5 bin kişi olur, 10 bin kişi olur, nasıl olursa Türkiye'nin bir savunma gücü olması lazım ve önüne gelenin Türkiye'ye "Ben şu kuruma saldırıyorum, bu kurumu çökertiyorum, işte şurada şunu yapıyorum." diyememesi lazım, derse de sonuç alamaması lazım. Sonuç itibarıyla böyle bir durum var. Ulusal koordinasyon kurulu öneriyoruz biz. Ulaştırma Bakanlığımıza da bu öneriyi götürdük. Bu ulusal koordinasyon kurulunda devletin, üniversitelerin, sektörün

ilgili kişileri bir araya gelerek bu koordinasyon kurulunda Türkiye'nin politika ve stratejilerini belirlesin istiyoruz.

Teşekkür ediyorum Sayın Başkan.

BAŞKAN – Hocam, oldukça teferruatlı ama bir o kadar da ürkütücü sunumunuzdan dolayı teşekkür ediyorum.

Kaç asır önce söylendiğini bilmiyorum ama bu siber güvenlikle ilgili konu hep gündeme geldiği zaman bir söz var, hep o aklıma gelir: İnsanı yere yıkan, yumruğun sertliğinden ziyade nereden geldiği görülmeyen yumruktur." diye. Aslında belki de tam bu siber güvenlik konularını izah eden bir hadise.

Ben şimdi burada sizi dikkatlice dinledim, "Siber güvenlik strateji belgesi oluşturulmalı." diyorsunuz. Amerika, Hindistan, Hollanda, Almanya filan yayınladı… Bunlar böyle uluorta herkesin gördüğü strateji belgesi midir siber güvenlikle ilgili?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Evet.

BAŞKAN – O zaman kamuoyuyla paylaşılıyor bunlar, değil mi?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Evet, paylaşılıyor.

BAŞKAN – Bizim böyle bir çalışmamız var mı Türkiye'de?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Dernek olarak uzman grubu arkadaşlarımızla çalışma yaptık belirli bir noktaya, bunu tabii ki Ulaştırma Bakanlığımızla da koordine ediyoruz ama Başbakanlığımız marifetiyle bu strateji belgesinin yayınlanması lazım. Önümüzdeki etkinlik sonrası 18 Haziranda sırf bununla ilgili bir toplantı yaparak bu strateji belgesini hazır hâle getirip Bakanlığımıza sunmayı planlıyoruz.

BAŞKAN – Yetkili kurum kim olmalı sizce? Mesela Amerika'da kim yetkili kurum? "Obama" dediniz…

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Amerika'da NSA gibi, vesaire gibi birçok farklı kurum var. Yalnız şöyle bir şey var bu tür şeylerde, bir tane yetkili kurum tutmuyorlar özellikle. Mesela bu konuda 16 tane kuruluş var Amerika'da çalışan ve üstelik 16'sı da farklı görevler üstlenmiş; kimi legal, kimi illegal, kimi başka türlü faaliyetler yürütüyor. Ama bizim Türkiye olarak böyle 16 kuruluş olması gerekmiyor, ilk etapta yapmamız gereken bir düzenleyici olabilir, bir Başbakanlık bünyesinde olabilir, bir bakanlığımız bünyesinde olabilir ama Türkiye'nin politika ve stratejilerini üretecek, bir de siber savunma gücünü oluşturacak. İlk etapta dediğimiz bu.

BAŞKAN – "Haydi" dendiği zaman kim önce hemen üzerine alınacak yani?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Onun biz bir türlü cevabını bulamadık. Bunu Ulaştırma Bakanlığımıza götürdük, İçişleri Bakanlığımıza götürdük, Adalet Bakanlığımıza götürdük, Millî Savunma Bakanlığımıza götürdük, BTK'ya, TÜBİTAK'a götürdük ama maalesef bir inisiyatif alıp birinin "Bu işin otoritesi benim." demesi lazım. Şimdi, TÜBİTAK bir

tarafta çalışıyor, BTK bir tarafta çalışıyor, emniyet bir tarafta çalışıyor, bakanlıklar bir tarafta çalışıyor biz de doğrusu bilmiyoruz bunun kim olması gerektiğini.

BAŞKAN – Son bir şey daha sorup hemen üyelerimize söz vereceğim.

Millî bir host alt yapısı oluşturalım projemiz var, dünya yaptı biz de yapabiliriz. Bu projeyi yapan kim?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN - Biz yaptık arkadaşlarla beraber, bir grup arkadaşla. Ana posta dedik adına, Türk posta dedik, böyle bir posta altyapısı, bir test aşamasında oluşturduk, bunun yazılımını vesairesini ama bunun tabii uygulamaya geçmesi ciddi kaynak isteyen bir durum ve bunun da işletilmesi de ciddi kaynak gerektiren bir durum. Amerika şöyle yapıyor: Bu devletin kontrolünde ama bunu devlet yapmıyor. Diyor ki X şirketine mesela daha önceki sunumlarda size anlatıldığını biliyorum ben, işte alan hatları sağlayıcısı ICEN diye bir kurum, diyor ki dünyadaki alan hatlarını ben şey yaparım diyor. Amerika'da bir başka kurum çıkıyor, diyor ki…

BAŞKAN - Amerika örneği doğru bir örnek değil Hocam. Amerika internetin sahibini kendisi olarak gören bir ülke. Amerika'dan örnek vermeyin Almanya'dan verin mesela, Fransa'dan verin.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Mesela Çin, Almanya, Kore, Japonya kendi posta altyapılarını oluşturdu ve devlet içerisindeki bütün şeylerini de bu kendi posta altyapılarıyla konuşuyor. Örnek olsun diye söylüyorum, mesela bir Japon vatandaş Türkiye'ye geldiğinde kendi şirketinin dışında hotmaili, gmaili, yahooyu kullanması işten atılma sebebidir. Yani o şey üzerinden paylaşamaz.

Sonuç itibarıyla biz devlette kendi posta altyapımızı oluşturalım, o posta altyapısı üzerinden paylaşalım diyoruz. Nitekim bir çalışma yaptık biliyorsunuz BTK olarak. Ben aynı zamanda on iki yıldır BTK Başkan Yardımcılığı görevi yürüttüm ve bir ay oldu ayrılalı. Orada kayıtlı elektronik posta dediğimiz sitemi bunun için hayata geçirdik. O şuydu: Kendi millî posta altyapımızı oluşturduğumuzda onun üzerine de kayıtlı elektronik postayı koyduğumuzda şunu yapacaktık: O posta kendi haberleşme altyapı üzerinden tüm attığımız mailleri ve maillerle birlikte paylaştığımız resmî belgelerimizi, eklerimizi kayıtlı elektronik postayla yaparak kendi iç döngümüzde bütün bilgilerimi, belge paylaşımımızı gerçekleştirecektik, şimdi o yasalaştı, çok önemli bir adım ama altı boş kaldı. Biz bu kayıtlı elektronik postayı nereden dolaştıracağız yani postalarınızı, belgelerimizi, resmî yazışmalarımızı? Mutlaka bir posta altyapısı üzerinden oluşturacağız. İstiyoruz ki onu biz kendi millî altyapımızdan yapalım yani gmailden birbirimize mail atmayalım, hotmailden atmayalım ya da herkes kendi kurumundan atıp böyle farklı farklı olmasın. Adını gmail gibi, hotmail gibi, yahoo gibi işte Türk posta bilmem ne posta koyalım.

BAŞKAN – Biz post'u arkasına bir a harfi ekleyerek posta yaptık. Host'u da arkasına bir a harfi ekleyerek hotsa yapsak ama bu sefer de hotsa zincirleri var ondan belki isim hakkı almamız lazım.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Evet Başkanım.

BAŞKAN – İşin latifesi bir yana, bunu yapmak lazım.

Buyurun Sayın Doğru.

REŞAT DOĞRU (Tokat) – Hocam çok teşekkür ediyorum. Dehşetle dinledik, harika bir konuşma, sunum yaptınız. Sunumla ilgili o sunum bizde yok, bize verdiğiniz şeyler içerisinde.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Mail ortamında göndereceğiz.

REŞAT DOĞRU (Tokat) – En azından onun elimizde bulunmasında çok büyük fayda olacağı kanaatindeyim.

Ben bir iki konuyu bilgilenme noktasında sormak isterim.

Anladığımız kadarıyla yani artık böyle büyük ordulara falan gerek yok yani silahlı güçlere yani siber orduyu kurduğunuz zaman herhâlde bu işte epeyi bir mesafe almış olacaksınız. Türkiye'de şu anda bu siber ordu dediğiniz veya hackerlar dediğiniz onlarda bizim kaç elemanımız var? Türkiye'de kaç kişi bu işlerde çalışıyor? Birinci sorum bu.

İkincisi, tabii Türkiye Cumhuriyeti Devletinin istihbarat bölümü MİT'te bulunuyor. MİT'te sizin bu dediğiniz siber orduyla ilgili bir çalışma var mı, grup oluşturulmuş mu? Gizli bilgi mi bilmiyorum ama, herhalde gizli bilgi değildir.

Üçüncüsü de, malumunuz olduğu şekilde Amerika Birleşik Devletlerinde İkiz Kulelere bir saldırı yapıldı. Bu saldırıda insan kaynağı kullanılmadığı fakat bilgisayarların yönlendirilmesiyle bunun olduğu şeklinde söylemler var. Yani buna katılıyor musunuz? Bununla ilgili ne söylemek istersiniz, onu öğrenmek isterim.

Siber güvenlik strateji dediniz bununla ilgili de Türkiye Cumhuriyet Devletinde şu anda durum nedir? Bununla ilgili bilgi istiyorum.

Teşekkür ederim.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Birincisi Türkiye'de hacker sayısının çok olduğunu biliyoruz ve çok iyi yetişmiş elemanlar.

BAŞKAN – Çok dediğiniz rakam nedir mesela?

REŞAT DOĞRU (Tokat) - 100 bin kişi var mı?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Yok, o kadar yok. Yani buradan şunu söylemeye çalışıyorum: Bu da şöyle bir şeydir tabii nitelik burada çok önemli. Yani bir sayfayı göçertmek hackerlik değil. Ama şunu biliyoruz Amerika geçenlerde bir yarışma yaptı biliyorsunuz bir şeye erişme noktasında. Bir metin içerisine bir şey gizledi "Bunu kim bulacak?" dedi, İstanbul'dan bir tane çocuk buldu dünyada ve dünya birincisi oldu. Şimdi bu şunu gösteriyor ki, bütün dünyada özel eğitim aldıkları…

BAŞKAN – Saat farkından birinci olmadı değil mi?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Yok Başkanım.

Ve nitekim şimdi de bu arkadaşımız Amerika'da doktora yapıyor. Burada şunu söylemeye çalışıyorum. Bir nitelik var burada. Sizin nitelikli 100 tane elemanınız olur diğerinin 10 bin tane elemanına bedeldir. O oturur bir yerde, o 10 bin tanenin yaptığını yapar ama arkadaşlar çalışıyorlar. Şunu söyleyeyim:

Mesela önümüzdeki toplantıda bu konuda Bir de şöyle bir sıkıntımız var. Bu konuda bir politikamız olmadığı için, işte beyaz şapkalı, siyah şapkalı, gri şapkalı diye nitelendiriyorlar, korkularından, kaygılarından bu arkadaşlarımız da çıkıp biz bu işin uzmanıyız diyemiyor. Bir de şöyle bir sıkıntı var. Bu konuda eğitim de alamıyorlar. Eğer eğitim alıp sertifika alırlarsa bu arkadaşlar, uluslararası sertifika o zaman yurtdışına giriş çıkışlarında vize konusunda acayip sıkıntı yaşıyorlar, bir de böyle bir durum var. Yani sonuçta kimse sertifika almak istemiyor. Uluslararası sertifikayı alanlar belli oluyor. Dolayısıyla burada bir sahaya belirlemek oldukça zor bir durum ama şunu söylemek lazım, bizim…

REŞAT DOĞRU (Tokat) - Yani siber ordumuz var mı Hocam?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Şöyle söyleyeyim, siber ordu ancak şöyle olur: Organize bir hareket hâline getirirsen bu insan kaynağını siber ordu olur ama kimin, nerede, ne yaptığı belli olmayan, belki Türkiye'yi savunuyorum diye gider bir siteyi çökertir, Türkiye'ye zarar verir. Öyle tehdit ve tehlikeler de var, kontrol dışı bu insanlar.

BAŞKAN - Nitekim öyle hackerler var mesela, bayrağımızı falan kullanan.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Bayrağımızı kullanıyor, internete logolar atıyor. Bu uluslararası devlet ilişkilerine de ciddi zarar verebilecek şeyler de yapılabilir.

REŞAT DOĞRU (Tokat) - Bölücü terör örgütüyle ilgili, diğerleriyle ilgili bayağı saldırı olmuştu yani.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Ferdi ve fevri şeyler oluyor. Bu organizasyonla bizim bu Ulusal Koordinasyon Kurulundan üç tane çözüm önerdik. Birincisi dedik ki bu politika ve strateji belirleyen bir grup oluşsun. İkincisi, bir uzmanlar grubu oluşsun, bu sizin söylediğiniz bir ordu olsun. Bu illaki savaş yapsın, saldırsın değil, bize karşı saldırılara karşı bir savunma gücü oluşturalım. X kurumuna saldırı yapıyorum dediğinde atıyorum any mouse, Wikileaks, x, y, z biz o arkadaşları o kuruma destek ekibi olarak verelim ve o savunma gücü oluşsun. Üçüncüsü de üniversitelerde çok ciddi şekilde bir güvenlik çalışması yapan hocalarımız var. İşte Ali Beyler ASELSAN'da yapıyor, dünyanın en kritik kriptolarını üretiyorlar. ODTÜ'de …, Şeref Hocam dünyada ödül almış hocalarımızdan bir tanesi bu konuda işte parmak izinden yüz tanıma projesiyle dünyada ödül aldı. Bu konuda alanında hakikaten dünyada isim olmuş birisi Şeref Sağıroğlu. Üniversitelerde böyle hocalarımız ve sektörde de böyle uzmanlarımız var. bu uzmanlardan oluşan da bir grup oluşturalım. Bunları da bizim bilgi güvenliği kripto algoritma ARGE altyapımızı oluştursunlar istiyoruz. Bunları yapacak olan da bu Ulusal Koordinasyon Kurulu dediğimiz kurul. Bir an önce bunun hayata geçmesi lazım.

İkiz Kule, katılıyorum. Bizim birçok bilmediğimiz şeyler siber savaşlarla yapılıyor, bunun da bunlardan biri olma ihtimali çok yüksektir. MİT gibi, Emniyet gibi kuruluşlarımız bu konuda iyi yetişmiş elemanları var, yetiştirmeye de çalışıyorlar, eğitimleri de alıyorlar. Strateji Eylem Belgesi noktasında da dediğim gibi bir an önce çalışma yapıp bunu hayata geçirmemiz gerekiyor. Şundan gerekiyor: Kurumda çalışan arkadaşlarımız bilmiyor. İşte geçen ki şey ne oldu? Şifre 123456 dedi. Strateji Eylem Belgesinde demesi lazım ki somut bir örnek olsun diye şifreler bir, nümerik, alfa nümerik şu şu karakterlerden, şu kadar BİT olması lazım atıyorum ve kurum da çalışanlar da öyle 123456 diye şifre vermemesi lazım, basit bir örnek. Yani

atıyorum sistem altyapılarının şu şekilde olması lazım. Strateji belgesi bütün kurum ve kuruluşlara bir mecburiyet getirecek, zorunluluk getirecek, hiç olmazsa kurumlar bu strateji belgesinden sonra istese de istemese de Başbakanlık böyle istedi diye güvenlik altyapılarını belirli bir seviyeye getirmiş olacaklar, strateji belgesi de böyle bir şey.

REŞAT DOĞRU (Tokat) - Bir şey daha sorayım. Şu Bilgi Güvenliği Derneği deniyor ya. Mesela Şeref Hocam falan tanıyordu. Şimdi bu Güvenlik Derneği olarak kendiniz yani illa birisinin resmî görev vermesi gerekir mi yani böyle bir şey oluştursanız bu mahsur mu teşkil edebilir?

BAŞKAN - Bir STK'nın falan ona gücü yetmez yani sonuçta uyarıcı görevini yapar ama onların bir organizasyon yapması zor.

REŞAT DOĞRU (Tokat) - Bu tür şeylere destek veriliyor Sayın Başkanım yani. Mesela devlet destekleyebilir yani illa burada….

BAŞKAN – Ben onu soracağım. Siber ordu oluşturuyor diye.

Mehmet Bey, herhalde sen benzer bir şey soracaksın.

MEHMET S. TEKELİOĞLU (İzmir) – Şimdi bu kurulan siber ordular tek merkezden mi ülkenin tüm altyapısını savunuyorlar, kuruyorlar? Nasıl bir mekanizma kuruyorlar? Mesela atıyorum Amerika Birleşik Devletlerinde birkaç yıl önce çok ciddi bir elektrik kesintisi yaşanmış. Hiçbir şey yokken birden hatta üç gün falan sürdü yaz, çok sıcak, hastanelerde de sorun yaşandı ve elektriği bir türlü veremediler, iki, üç gün sürdü bu. Sonra çözebildiler sistemi. Onu sorgulamaya başladılar elektrik altyapısında problem mi var vesaire mi diye. Mesela New York eyaletini düşünelim bunlar kendi kurulan ordular belli sayılarda mı dağıtılıyor yoksa merkezî bir noktadan ülkeye girişleri kontrol altına mı savunma yapabiliyorlar? Bir de siber orduyla alakalı bizim Türkiye'nin herhangi bir hazırlığı yok falan dediniz ama yani şöyle üç hafta öncesinde veya iki hafta öncesinde basında bir haber geziyordu "Millî İstihbarat Teşkilatı siber ordu kuruyor." diye. Bununla alakalı var mı herhangi bir bilginiz? Sizden istifade edildi mi bu konuda? Görüşmeleriniz oldu mu?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Şöyle, birinci soru Amerika örneği verdiniz, Başkanım da Amerika haklı olduğu gibi farklı bir şey ama on altı farklı kurum var ama Amerika'da on altısı da sonuçta bir merkeze bağlı. Bir merkez on altı kurumun politika ve stratejisini belirliyor. Başka kurumlarda, ülkelerde işte İngiltere'de, Japonya'da, Çin'de yine benzer şekilde ayrı ayrı birimlerde oluşturulmuş siber ordular var ama biri şunu yapıyor. Diyor ki: "Eğitimini ben üstleniyorum." "Beş bin tane, on bin tane, yirmi bin tane uzman yetiştireceğim." diyor. Üniversitede enstitü kurmuş. Birileri alıyor bu uzmanları şuralarda istihdam edeceğim diyor. İşte askerî alanda, askerî savunmada bunları kullanacağım. İşte istihbaratta bunları kullanacağım. Sonuçta yine devlet otoritesi bunların planlamasını, koordinasyonunu politikasını bir otorite belirliyor. Genelde böyle uygulamalar. Bizde de biraz önce söyledim, MİT'in de bu konuda çalışması var, Emniyetin de çalışması var. Kurumlarımızın da benzer çalışmaları var ama bir koordinasyon ve organizasyon eksikliği var. Bizim burada söylemeye çalıştığımız Türkiye'de bu anlamda bir koordinasyon merkezinin mutlaka olması lazım, önerimiz o doğrultuda.

REŞAT DOĞRU (Tokat) – Kanun olarak…

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Evet. Mesela siber devlet yasa tasarısı diye bir tasarımız var bizim. Boş duruyor henüz daha gündeme gelmedi bir türlü.

BAŞKAN - Kim çalışıyor?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Adalet Bakanlığında duruyor Sayın Başkanım. Kanunlar Kararlarda da olabilir belki öyle hatırlıyorum.

İkincisi kişisel verilerin korunma yasa tasarısı var. biliyorsunuz aşağı yukarı on yıldır, on beş yıldır duruyor. Birinci yasal boşluklar. Şimdi biz Barolar Birliğiyle siber güvenlik hukuku çalıştayı yaptık. Onlarla böyle bir kanun çalışması hazırlığı yapalım, sizlere sunalım diye ama bu iki yasa birinci öncelikli yani siber devlet yasa tasarısı ve kişisel verilerin korunması yasa tasarısı. Bir de yasal boşluğumuz var bizim. Bir yasal boşlukların giderilmesi lazım. iki, kurumsal anlamda düzenleyici bir otorite oluşturulması lazım. Bir de farkındalık olayı. Tabii üç temel problem var.

BAŞKAN – Buyurun.

MEHMET S. TEKELİOĞLU (İzmir) – Bu kişisel verilen korunmasıyla ilgili kanun bildiğim kadarıyla Adalet Komisyonunda gündemde. Uyum komisyonu olarak onun bize de geleceğini bekliyorduk ama henüz bir şey çıkmadı.

Ben bir şeyi merak ediyorum.

BAŞKAN – Sayın Tekelioğlu, AB Uyum Komisyonu Başkanı.

MEHMET S. TEKELİOĞLU (İzmir) – Şunu merak ediyorum: Çeşitli uzantılar var şeyden sonra gov gibi, com gibi, edu gibi, org gibi. Mesela sizin de bilgigüvenligi.org.tr olarak kullanıyorsunuz. Bunlar arasında bir güvenlik sıralaması yapılabilir mi yani şu daha güvenlidir.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Yok hayır hiç ilgisi yok güvenlikle.

MEHMET S. TEKELİOĞLU (İzmir) - Bunların hepsi neticede Amerika'da bir yerde işleniyor mu diyelim.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Kısmen evet diyebiliriz.

MEHMET S. TEKELİOĞLU (İzmir) - Şöyle bir sorun: Şimdi siz dediniz ki Hotmail, gmail kullanılıyor. Bu doğru değil. Fakat öbür taraftan da kurumların mail adreslerini kullandığımız zaman oralarda da müthiş bir sınırlama var.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Çok doğru.

MEHMET S. TEKELİOĞLU (İzmir) – Yani dolayısıyla bizi mecbur ediyor bir yerde bu çünkü sizin iradeniz dışında sizin mailinize birisi çok yüksek kapasiteli bir mail gönderiyor, onu anlık fark edemiyorsanız, silemiyorsanız o sizi tıkamış oluyor. Dolayısıyla da hotmail ya da gmail ya da benzeri şeyleri kullanmak zorunda kalıyoruz. Bunun bir çaresi var mı görünürde?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Var. Bizim mesela bütün kurumlar isterlerse bu kapasiteyi çok rahat artırabilirler, kota dediğimiz şey. Her bir kullanıcıya…

MEHMET S. TEKELİOĞLU (İzmir) – Yani artırmıyorlar ama yani benim var şimdi bu tür bir şeyim yani çok istedim ki sürekli oradan kullanayım ama bu kota sıkıntısından dolayı mecbur oldum gmaili kullanmaya.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Doğru çünkü en iyi yönetilen posta altyapısı orası ne yazık ki. Doğru böyle bir şey, bu gerçek.

MEHMET S. TEKELİOĞLU (İzmir) – İkincisi ben pazar günü bu siber saldırılardan birine maruz kaldım. Facebook hesabıma maalesef girdiler ve bütün oradaki gruplara para talebi, kontör talebi, kredi kartı talebi. Beni tanıyanların pek çoğu böyle bir şey yapmayacağımı bildiği için buna itibar etmemiz ama üç, beş kişi de duydum kimi kredi kartına para göndermiş kimi kontör göndermiş vesaire. Ama orada ben bir hata yapmışım bunu sonrada fark ettim. Ben facebook'taki hesabın şifresiyle mail adresinin şifresini farklı yapmamışım. Ama bu konuda beni uyaran da olmadığı için şimdi bunu deneyerek öğrenmiş oldum. Hakan Bey ilgilenecek sağ olsun. Bu tür sorunları yaşıyoruz tabii ki yani.

Bir de depolama sıkıntılarından dolayı da bu gmail'i, hotmail'i kullanma durumunda kalıyoruz. Çünkü artık yanımızda eskiden dosya taşıyorduk ondan geçtik şimdi flash bellek bile taşımak istemiyoruz. Dolayısıyla oraya koyuyoruz, bir şey olunca oradan şık diye arayıp buluyoruz yani. Bu sorunların bizim kurumlarımız içerisinde çözülmesi belki emniyet bakımından daha mı iyi bilmiyorum yani.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Bizim önerimiz özellikle devlet yazışmaları ve bilgi, belge paylaşımının tamamen kapalı ortamlarda ve millî altyapılarla yapılması yönünde. Bunu yapmadığımız sürece devlet sırrından bahsetme şansımız yok Sayın Başkanım çünkü hepimizin oradaki bütün konuşmaları, twitt'teki, youtube'taki, facebook'taki ve gmail'deki her türlü bilgilerimiz dışarıya açık demektir. Sonuçta bunlar içerisinde çok önemli devlet bilgileri, devlet görüşmeleri, bilgi paylaşımları olabilir. Bunların bizi nereye götüreceğini bilmiyoruz ne yazık ki.

MEHMET S. TEKELİOĞLU (İzmir) – Affedersiniz Başkanım, küçük bir sorum olacak.

BAŞKAN – Buyurun.

MEHMET S. TEKELİOĞLU (İzmir) – Bizim mesela Türkiye Büyük Millet Meclisinin bilgi işlem sistemindeki bilgiler burada mı depolanıyor Amerika'da mı depolanıyor?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Burada depolanıyor.

MEHMET S. TEKELİOĞLU (İzmir) – Yani hiç Amerika'yla bizim ilgimiz yok mu?

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Yok.

MEHMET S. TEKELİOĞLU (İzmir) – Dolayısıyla emniyetli mi yani burası?

BAŞKAN – Peki şöyle bir şey oluyor yalnız Mehmet Ağabey. Şimdi bu gmail, hotmail, yahoo vesaire gibi şeyler kullandığınız zaman dünyada başka yerlerde mesela her yerde ona uygun bir şekilde ve hızda

ulaşıyorsunuz fakat diğer servis sağlayıcıları kullandığınız zaman dünyanın başka mekânlarında onu rahatlıkla kullanamıyorsunuz, böyle bir sıkıntı da var. Yani o gmaili kolaylaştıran veya yahooyu kolaylaştıran sadece depo alanının genişliği değil. Aynı zamanda hızla da ulaşabilmemiz.

MEHMET S. TEKELİOĞLU (İzmir) – Kaldı ki tr uzantısı olunca birçok yerde sıkıntı yaşıyoruz.

BİLGİ İŞLEM BAŞKANLIĞI YARDIMCISI HAKAN YILDIRIM - Sayın Başkanım, bir de kapasite konusunda şöyle bir problem de var: Biz malumunuz Kamu İhale Kanunu'na tabiyiz. Yani bu kapasite konusunda önümüze bir şey çıktığı zaman yedi sekiz ayda onu ancak ikmal edebiliyoruz ama öbür taraf sınırsız kapasite veriyor, haklılar. Bir de sayın vekillerimiz birçoğunda şu endişe de var: Yani benim burada dönemim bittiği zaman daha evvel şöyleydi ertesi gün hesap kapatılıyordu. Çok yanlış. Yani bunu zor ikna ettik ki dursun, en azından eski vekillerimizin dursun. Halbuki şöyle de bir şey var yani kapasite olarak burada bir sorun da teşkil etmiyor bu.

MEHMET S. TEKELİOĞLU (İzmir) – Yani affedersiniz lokantayı kullanabiliyor da şeyi niye kullanamıyor yani o mail uzantısını niye kullanamıyor yani? Ne kadar saçma bir şey ya. Gerçekten böyle mi?

BİLGİ İŞLEM BAŞKANLIĞI YARDIMCISI HAKAN YILDIRIM - Aynen böyleydi. Değişiyor şu anda.

MEHMET S. TEKELİOĞLU (İzmir) – Yani lokantadan daha mı değersiz yani mail uzantısı?

BAŞKAN – Neyse hallolmuş artık, kızma yani.

BİLGİ İŞLEM BAŞKANLIĞI YARDIMCISI HAKAN YILDIRIM – Şöyle bir örnekle de karşılaştım. Hem Mehmet Başkanımızın hem sizin e-postalarınızla uğraşırken şunu fark ettim yani bunu da belki dile getirmekte fayda var. Mehmet Başkanıma şifresini verirken dedim ki: "Egendim bu şifreyi değiştirin." O da bana gülerek baktı, dedik ki: "Zaten neyim olsa görebilirsiniz siz. Niye değiştireyim ki?"

MEHMET S. TEKELİOĞLU (İzmir) – Değiştirdim, değiştirdim.

Ne yaparsam yapayım siz nasıl olsa buna vâkıf olmak isterseniz olursunuz, demek istediğim o.

BAŞKAN - Gazeteci arkadaşın aynı şeyi olmuş Mehmet Ağabey. Arkadaşları demiş ki: Vah vah. İsmini de söylemeyeyim Muzaffer Bey biliyor. Yani bu kadar düştü mü yani bu kadar kontör isteyecek kadar falan diye.

BİLGİ İŞLEM BAŞKANLIĞI YARDIMCISI HAKAN YILDIRIM - Başkanım yani ben burada bir psikolojiyi anlatmaya çalıştım. Şöyle oluyor yani kurumlarda görüyoruz biz bunu. Diyorum ki: Gmaile daha mı çok güveniyorsunuz? Yani ben bunlarla karşılaşıyorum, bu konuyla. Daha mı çok güveniyorsunuz diyorum? Şöyle diyor: Yani bu bilgi burada kıymetli. Mesela benim attığım şeylerden bazıları maillerde burada bir kıymet teşkil ediyor. Gmail için bir kıymet teşkil etmiyor bu diyor. Onun için yani insanların Mustafa Bey'in de ben o konuda dikkatini çekmek istiyorum. Gmaili, yahooyu kullanırken biz burada görüyoruz yani biz bunun mücadelesini vermeye çalışıyoruz. Niye kullanıyor? Yöneticilerle de bir müddet şeyini verdik. Meclis TV gmail üzerinden görev dağılımını yapmıştı yani buraya hangi kameramanın geleceği, hangi muhabirin geleceğine gmaille yapıyordu ta ki bu yeni e-posta sistemi kuruluna kadar. Kurulduktan sonra artık orada yapıyor.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN –Sayın Başkanım, biz bu millî posta altyapısını gündeme getirdiğimizde medyada, kamuoyunda şöyle bir algı

oluştu: "Bizim cep telefonlarımız, telefonlarımız dinleniyor, şimdi de postalarımız dinlenecek." diye. Olay çok farklı boyutlara çekildi, maalesef. Bir de böyle bir bizim şeyimiz var.

BAŞKAN – İşte yani erişkin eğitimi her zaman zordur ama Hocam.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Kesinlikle

BAŞKAN - Çocuk eğitiminden daha ziyade zordur. Bizim mutlaka bu dijital okur-yazarlık noktasında ciddi bir çalışma yapmamız lazım.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Olay bu kadar basite indirildi kamuoyunda. Ne yazık ki destek görmesi gerekirken bu kadar önemli bir husus böyle algılandı.

BAŞKAN – Hocam biz bunları yani anlattığınız konuları gerçekten çok önemsiyoruz yani ürkütücü ama çok çok önemsiyoruz. Daha teferruatlı bilgileri komisyonumuza sunarsanız biz komisyon raporumuza onları kaydederiz.

BİLGİ GÜVENLİĞİ DERNEĞİ YÖNETİM KURULU BAŞKANI PROF. DR. MUSTAFA ALKAN – Rapor hâlinde size sunacağım.

BAŞKAN – Memnuniyetle onları yaparız.

Bir duyuru yapalım sonra toplantıyı bitirelim.

17-18 Mayısta ODTÜ'de Beşinci Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı yapılacak. Ben de Bilişim ve İnternet Araştırma Komisyonu Başkanı olarak böyle bir açılış konuşması talep etmiştim. Teklif gelmişti. Katılacağız ama hep beraber katılırsak ODTÜ'de, 17 Mayıs, saat 10.00'da açılışı var, üyelerimizi davet edelim.

Bu arada arama konferansıyla ilgili duyuruyu yapacağız ama Aykan Bey burada, Reşat Bey burada başka bizim komisyon üyesi kimse kalmadı. 25, 26, 27 Mayısta İstanbul'da arama konferansı ve yoğun bir ziyaret trafiğimiz olacak. Cuma, cumartesi, pazar. Cuma günü ziyaret, cumartesi günü öğlene kadar ziyaret, öğleden sonra ve pazar günü tam gün ama biraz yoğun da çalışacağız spor kıyafetiyle özelikle katılmanızı rica ediyoruz, rahat bir kıyafetle. Yoğun bir arama konferansı yapacağız, çok faydalı bir toplantı olacağını düşünüyorum yani çok fazla paydaşı bir arada getireceğimiz çok güzel bir toplantı olacak. Yani 25, 26, 27 Mayısta böyle bir şey var. Yarın da Telekom'un bir ziyaretini planladık ama bilmiyorum siz de uygun görürseniz Türkiye'de internet trafiğini bizzat görebileceğimiz bir mekân, saat 10.00'da böyle bir ziyaretimiz var. Çok faydalı olacak. 10.00'la 12.00 arasında herhalde 11.30 arasında ziyaret yapacağız.

Kapanma Saati: 13.54