**TÜRKİYE BÜYÜK MİLLET MECLİSİ**

| YASAMA DÖNEMİ | YASAMA YILI |
| --- | --- |
| 24 | 3 |

# (10-74)- HABERLEŞME ÖZGÜRLÜĞÜNE VE ÖZEL HAYATIN GİZLİLİĞİNE YÖNELİK İHLALLERİN TESPİTİ VE ÖNLENMESİNE İLİŞKİN TEDBİRLERİN BELİRLENMESİ AMACIYLA KURULAN MECLİS ARAŞTIRMASI KOMİSYONU

## TUTANAK DERGİSİ

***6 Mart 2013 Çarşamba***

**(10-74) – HABERLEŞME ÖZGÜRLÜĞÜNE VE ÖZEL HAYATIN GİZLİLİĞİNE YÖNELİK İHLALLERİN TESPİTİ VE ÖNLENMESİNE İLİŞKİN TEDBİRLERİN BELİRLENMESİ AMACIYLA KURULAN MECLİS ARAŞTIRMASI KOMİSYONU**

**GÖRÜŞME TUTANAKLARI**

**6 Mart 2013 Çarşamba**

----0----

**K O N U**

**Sayfa**



**İ Ç İ N D E K İ L E R**

**Sayfa**

| | | |
|---|---|---|
| Yılmaz TUNÇ | (Bartın) | 14, 17, 19, 20 |
| Ali ERCOŞKUN | (Bolu) | 16, 22, 31:32 |
| Mihrimah Belma SATIR | (İstanbul) | 20 |
| Hasan Ali ÇELİK | (Sakarya) | 22 |
| Enver ERDEM | (Elâzığ) | 32, 34 |

**Açılma Saati: 11.01**
**Kapanma Saati: 13.05**

BİRİNCİ OTURUM

6 Mart 2013 Çarşamba

Açılma Saati: 11.01
BAŞKAN: Zeyid ASLAN (Tokat)
BAŞKAN VEKİLİ: Yusuf BAŞER (Yozgat)
BAŞKAN VEKİLİ: Öznur ÇALIK (Malatya)
SÖZCÜ: Yılmaz TUNÇ (Bartın)
KÂTİP: Mihrimah Belma SATIR (İstanbul)

_____0_____

BAŞKAN – Değerli arkadaşlar, bugünkü gündemimizde Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Üyesi ve Fen Bilimleri Enstitüsü Müdürü Sayın Profesör Doktor Şeref Sağıroğlu'nun "Haberleşme ve Özel Hayatı İhlal Edebilecek Teknolojiler" konulu sunumu olacak. Ayrıca Teknoloji Enstitüsü Müdürü Mustafa Hocamız da gelecekti ama rahatsızlığı sebebiyle kendi sunumunu da "Değerli Hocamıza benim adıma da bizim sunumumuzu da kendisi yapacak." diye bize iletti.

Yani Hocam, siz iki sunumu birden birleştirerek beraber yapmış olacaksınız. Hazırsanız buyurun Hocam.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Başkanım, Mustafa Bey gelmek istiyor ama onu belki daha sonra… Bilmiyorum, nasıl planlandı. Ben sadece kendi bakış açımla onu anlatacağım.

BAŞKAN – Onu dün de arkadaşımızın görüşmesinde… O bir de dernek, Bilgi Güvenliği Derneğini de biz zaten şeyimize almıştık. Onu, Bilgi Güvenliği Derneğini temsilen ayrıca eğer rahatsızlığı… Herhâlde biraz kronik bir rahatsızlığı varmış mideyle ilgili.

Buyurun.

NAMIK HAVUTÇA (Balıkesir) – Evet, şimdi, Değerli Komisyon Başkanım ve arkadaşlarım; tabii, iki haftadır çalışıyoruz ve bayağı bir mesafe aldık. Kafamızdaki soruları yanıtlamak anlamında uzmanları dinliyoruz. Fakat şu ana kadar kafamızda böyle bir kanaate, oluşmuş bir bilgiye de maalesef ulaşamadık. Bununla ilgili biz ısrarla Komisyon üyesi arkadaşlarımız olarak diyoruz ki: Bu yasa dışı dinlemelerin en büyük muhatabı yargının kurucu unsurlarından olan avukat arkadaşlarımız. Dolayısıyla bu konuyla ilgili mağduriyetlerin yaratılmasında en sıcak bilgiye sahip olan, en derin bilgiye sahip olan avukatların, meslek örgütü olan Ankara Barosunun, özellikle Ankara Barosunun, Barolar Birliğinin ve İstanbul Barosu temsilcilerinin mutlaka, dinlenmesiyle ilgili bir karar alınmasını talep

ediyoruz, bu konulardaki uzman arkadaşlarımızın. Ben bunun Komisyonumuz tarafından öncelikle dinlenmesiyle ilgili bir karar olgunlaştırılmasını, bu kararla ilgili bir takvim oluşturulmasını talep ediyorum ve konuşmacı arkadaşımız da şöyle göz mesafemize geçerse… Ona da teşekkür ediyorum. Bunun uygun olacağını düşünüyoruz.

BAŞKAN – Teşekkür ediyorum.

Zaten yarın Türkiye Barolar Birliği sunumu olacak. Tabii biz Barolar Birliğinden kim gelecek… Yani şu anda bize bildirdikleri Başkan Yardımcısı. Tabii, Barolar Birliğinde bu konuda diğer avukat arkadaşlar yani kendi üyesi olan, Ankara Barosu, İstanbul Barosu, onlardan da temsilcilerle beraber katılabilir, onların da katkılarını burada sunabilir.

Bizim, tabii ki -şu anda, benim şahsıma da geliyor, mutlaka size de geliyordur- uygulamada savunma avukatlığı yapan birçok avukat arkadaşımız kendi davalarında yaşanan birtakım sorunları gündeme getiriyorlar ve bununla ilgili Komisyonun çalışma yapmasını istiyorlar ama bunu bizim görev süremiz içerisinde zaten ne tamamlayabilme şansımız olabilir… Çünkü çok sayıda bu konuda talep geliyor. Biz o zaman Komisyon olarak asli görevimizin dışına çıkar ve sadece mevcut birtakım bize müracaat edilen davaların incelemesine gireriz ki bu aynı zamanda biraz belki yasamanın yargıya müdahalesi olarak da düşünülebilir. Ama bu konuda uygulamada yaşanan yargı kararıyla yapılan yani yasa dışı dinleme ya da yargı kararıyla yapılan dinlemelerdeki aksaklıklarla ilgili uygulamanın içinde olan avukatları temsil eden barolar birliğini yarın zaten buraya davet ediyoruz.

Yarinki Barolar Birliğinin sunumundan uygulama hataları ya da eksikleri ya da yanlışlarıyla ilgili yeterli bilgi edinemezsek gerekirse bu konuda diğer barolardan veya bizatihi uygulamada çalışan avukat arkadaşlardan talebimiz olabilir ama yarınki gündemimizde Barolar Birliği var. Barolar Birliğini bir dinleyelim, bakalım sunumlarına eğer bu konuda yeterli olmadığını düşünürsek diğer barolardan da bu konuda talepte bulunabiliriz ama yarın zaten gündemimizde Barolar Birliği var. Bir önce arkadaşlarımızı, Barolar Birliğini dinleyelim, ona göre ihtiyaç duyarsak burada beraberce karara bağlarız.

Yarın, ayrıca, zaten hem uygulama hem teoriyle ilgili bu konuda, yüksek lisansından beri bu konu üzerinde çalışan, yine, bir değerli öğretim üyesi ki aynı zamanda da uygulamanın içerisinde bir avukat olarak da bildiğim kadarıyla çalışıyor Ersan Şen Hoca. Hem avukat olarak da fiilen bildiğim kadarıyla birçok davalarda… İki dönem de ayrıca öğretim üyesi olarak yüksek lisansından beri de özel hayatın gizliliği ve son on yıl içerisinde de telefon dinlemeleri üzerine ağırlıklı çalışmasını yürüten biri olduğunu ifade ettiler. Yarın hem kurumsal yapı olarak Barolar Birliğinin hem bu konuda uygulama ve teoride çalışmış bir hukukçu arkadaşımızı dinleyeceğiz. Yeterli olmazsa yarınki toplantıdan sonra gerekirse bunu değerlendiririz.

Buyurun Hocam.

HASİP KAPLAN (Şırnak) – Yalnız, geçmeden, uygulama sorunları olarak Başkanım… uygulama sorunları var, bir de anayasal açıdan sorunlar var. Biz baroları dinleyeceğiz. Bununla beraber Yargıtay, Yargıtay Başsavcılığı ve Anayasa Mahkemesini dinlemek zorundayız çünkü AİHM süreci değişti, yeni Anayasa değişiklikleri sonucu bireysel başvuru konusu artık Anayasa Mahkemesine gidiyor ve Avrupa İnsan Hakları Sözleşmesi'nin en önemli maddeleri olan "8" kişilik haklarıyla ilgili, özel hayatın korunmasıyla, iletişimle ilgili konuların denetimi de orada yapılıyor. Bu açıdan avukatlar önemli, baro önemli ama bir de uygulama alanı olarak… Biz Adalet Bakanlığını dinledik. Adalet Bakanlığı idari bir makamdır, yürütmedir. Yargıyı da dinlememiz iyi olur. Bu konuda uzman arkadaşlar bir çalışma yaparlarsa…

BAŞKAN – Tabii, daha önce burada toplantılarda arkadaşlarımız ifade etmişlerdi. Tabii, süreç içerisinde bunu beraberce karara bağlarız. Yani Yargıtayda özellikle özel hayatın gizliliği ve haberleşme hürriyetini ilgilendiren davaların bakıldığı dairenin başkanını veya oradaki yetkili üyeyi çağırabiliriz çünkü uygulamanın sadece…

HASİP KAPLAN (Şırnak) – Evet evet, konulara girmeden, davalara girmeden konuşabiliriz yani.

BAŞKAN – Tabii tabii, şu an biz yarın uygulamanın savunma tarafındaki arkadaşlarımızın yani uygulamayla ilgili düşüncelerini… Ama tabii, bunun bir de karar mercisi tarafındaki yargının… Tabii bunun da en üst mercisi Yargıtay Başsavcılığı da belki kararların doğrudan hüküm kuran daire başkanı veyahut da o daireden onların görevlendireceği bir üyeyi programa alırız, almamız da gerekir.

HASİP KAPLAN (Şırnak) – Uygulama örnekleri önemli. 28 Şubatta Ankara DGM sınırsız sorumsuz yurt içinde ve dışında dinleme kararları vermiş, bunu yaşadık, gördük. Buna benzer kararlardan günümüze ne değişti? O açıdan çok önemli olacağını düşünüyorum hukuk boyutu açısından, teknik boyutunu zaten ayrıca…

BAŞKAN – Teşekkür ediyorum.

Görüntülü basın mensubu arkadaşlarımız görüntü almışlarsa kendilerine teşekkür ediyoruz.

Buyurun.

ERDAL AKSÜNGER (İzmir) – Şimdi, değerli arkadaşım söyledi ama şöyle bir durum var: Mesela Ankara Barosunda -benim, tabii, gördüğüm kadarıyla- daha öncesinde, kişisel verilerin ihlalleri konusunda çok ciddi bir akreditasyon yapmış bir kurul var. Aslında "bilişim hukuku" diye de geçiyor ama altında kişisel verilerin ihlalleri konusunda uzmanlaşmış kişiler… Bunlarla daha önce ben görüşmüştüm. Burada biz eğer uzman konusunda da ihtiyacımız olacaksa -Ankara'da olması açısından söylüyorum özellikle- uzman alabilirsek onlardan burada çok faydalı olacağına inanıyorum. Çünkü ICANN yani uluslararası veri güvenliği konusunda belki de çok önemli çalışmalara bütün dünyada imza atmış bir kurumla akredite durumda çalışıyorlar şu anda ve bize özellikle önümüzdeki dönemde yapılacak yazsalar konusunda çok ciddi katkıları olacağına da inanıyorum gördüğümüz kadarıyla.

Şu, uzmanlık konusunda da bir çalışma yapacak mıyız, daha önce konuştuğumuz konuda?

BAŞKAN – Şimdi, uzmanlıkla ilgili -daha önce de belirttik- tabii kamu kurum ve kurumlarından uzman talebi… Yani onun dışındaki sivil toplum örgütleri ya da odalar, meslek gruplarından… Tabii bu bir gönüllü çalışma olduğu için, herhangi bir ücret karşılığı olmadığı için şu ana kadarki uygulamalarda talep edilmemiş, talep edilen noktalarda da karşılık bulmamış, böyle bir uygulama, böyle bir teamül oluşmamış. Ama tabii ki bizim konumuz biraz geniş -bu noktada size ben de katılıyorum- yani biz faydalanabileceğimiz, yararlanabileceğimiz sivil toplum örgütleri, meslek odalarından arkadaşlar varsa gönüllü çalışmaları… Bunları talep edebiliriz.

ERDAL AKSÜNGER (İzmir) – Onlar zaten bu konuda gönüllü çalışan bir ekip oluşturduğu için söyledim.

Barolar da hemen hemen bir kamu niteliği taşıyor çünkü bir tarafından. Ben çok faydalı olacağına inanıyorum yani birebir görüşmelerimizde, işin nasıl yapıldığını, hukuksal sıkıntıların ne olduğunu çok iyi ezberlemiş, çok içselleştirmişler çünkü konuyu, son on yılda özellikle. Faydalı olacağını düşünüyorum ben.

BAŞKAN – O konuda yani isim varsa…

ERDAL AKSÜNGER (İzmir) – İsteyelim onlardan. Onların zaten kurulları var, bir 15-20 kişilik kurulları var. İçinden mutlaka bir iki kişiyi onlar kendileri belirler yani. Biz isteyelim onlardan, Ankara Barosundan, isterseniz böyle bir girişimde bulunabiliriz. Yani tabii bu Komisyon kararıyla alakalı bir konu.

BAŞKAN – Tabii, dün dilekçeniz geldi. Haftalık programı yaparken yarınki… Tabii, geçen hafta programı biraz yapmadan çabuk bitirmişiz, ben bir dışarı çıkmıştım o arada. Yarınki toplantıdan sonra yani toplantının, sunumların bitiminden sonra tabii, önümüzdeki ve bir sonraki haftanın programını yapacağız. Onu yaparken bunu da gündeme alalım, bunu da değerlendirelim inşallah.

HASİP KAPLAN (Şırnak) – Bizim sunduğumuz bir öneri vardı yazılı, uzman önermiştim…

BAŞKAN – İşte, onlar da aynı şekilde, dediğim gibi, sivil toplum…

HASİP KAPLAN (Şırnak) – Uzman arkadaşlar şöyle bir yazı hazırlasa… Gönüllü olarak çalışacakları için yazının Meclisten gitmesinde büyük yarar var. Bu önerdiğimiz 3 uzmanın gönüllü olarak toplantılarımızda çalışabileceklerini ifade eden bir yazı giderse resmiyete dökülmüş olur.

ERDAL AKSÜNGER (İzmir) – Bunun niye Ankara…

HASİP KAPLAN (Şırnak) – Hayır, benim ayrıca bir 3 tane uzman önerim vardı…

ERDAL AKSÜNGER (İzmir) – Gördüm ben…

HASİP KAPLAN (Şırnak) – Yazılı olarak sundum. Onların burada, toplantılarda araştırma…

BAŞKAN – Yarın bunların hepsini karara bağlayalım inşallah.

HASİP KAPLAN (Şırnak) – Mutlaka bir muhataplık olmalı. Yani benim gidip kişisel olarak "Hadi buyurun, gelin, gönüllü çalışın." demem doğru değil. Burada o zaman denetim olmaz, sınırlama olmaz. Onun için Meclisin komisyonunun bildirimiyle üyeler bildirmiştir. Yazıyla da bildirim yapılır. O yazıyla da giriş çıkışlarında kolaylık…

BAŞKAN – Tamam, yarınki gündemimize alalım bunu. Yarın inşallah bunu karara bağlayalım.

Hocam buyurun, önce kendinizi tanıtarak başlarsanız…

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Teşekkürler.

Evet, öncelikle, Sayın Başkanım, saygıdeğer milletvekilleri; teşekkür ederim nazik davetiniz için.

Ümit ederim, bugüne yapmış olduğum bilgi birikimini, deneyimlerimi sizlerle paylaşır ve ülkemizde de önemli olan bu konuya katkı sağlamış olabilirim diye düşünüyorum.

Şimdi, sunumu kısaca, neler anlatacağım, onları bir özetlemek istiyorum. Aslında, biraz terminoloji, tanımlar üzerinde biraz durduktan sonra bilgi çağında karşımıza çıkabilecek ihlallerin neler olabileceğini sizlerle paylaşacağım, korkularımızı paylaşacağım, gelecekte karşılaşabileceğimiz sıkıntıları paylaşacağım. Yapılan saldırıların karakteristiklerini biraz sizlere aktardıktan sonra özel hayatı ihlal eden, aslında, en büyük altyapıyı sağlayan casus yazılımlardan bahsedeceğim sizlere ve tabii ki casus yazılımlar ve akıllı telefonlar üzerine Komisyonunuza pek çok kurumun bilgi verdiğini, bu konuda demo yaptığını basından öğrendim. Bunlarla ilgili daha farklı bir bakış açısı sunmaya çalışacağım. Haberleşme ve özel hayatın gizliliği konusunda neler yapılması gerekiyor, kendimce bazı önerilerimi sizlerle paylaşacağım.

Şimdi, aslında özel hayatın pek çok boyutu olabilir ama ben daha çok bilgi boyutuyla baktığımda, ülkemizde bir terminoloji problemi olduğunu düşündüğüm için bunu koydum. Biz veri bilgi ve öz bilgi gibi kavramların biraz üzerinde doğru şekilde durmamız gerekiyor. Her şeye veri diyoruz, işlenmiş veriye bilgi diyoruz ama katma değeri olan, farklı değer ifade eden, deneyimi gösteren, deneyimi sunan, birikimi ifade eden varlıklara da öz bilgi diyoruz. Şimdi, bunları özellikle söylüyorum yani literatür tanımı bunun ispat ile veriden bilgiye, ölçme ile gerçeklikten veriye gibi, kavrayış ile, yine, bilgiden öz bilgiye dönüş gibi bir tanımımız olabilir. Şimdi, burada, bugün bir sunum olacağını bilmek bir veri ama bugün hangi salonda kimlere sunum yapacağımı bilmek, oda numarası, konuşmacıyı bilmek bir bilgi ama bugün anlatılanları kavramayı da bir öz bilgi olarak ifade ediyoruz. Bunları neden söylüyorum? Şunun için: Bilgileri eğer sınıflandırabilirsek özel hayatımızda da karşılaşabileceğimiz mesela "Bir cep telefonu numarası, bir bilgi midir değil midir; özel hayatımızı ihlal eder mi etmez mi?"yi daha iyi ayrıştırabiliriz. Bunun için bunu vurguladım. Yani haddim değil, sadece bilgilendirme amaçlı bunu ifade edeyim.

Şimdi, güvenlik diyoruz, güvenlik tarafına baktığımızda aslında başımıza gelebilecek her türlü tehdit ve tehlikenin önceden öngörülüp önlem alınmasına biz güvenlik diyoruz. Tabii ki buna bilgi güvenliği olarak baktığımızda da elektronik ortamda sahip olduğumuz bilgi varlıklarının, kişisel bilgi varlıklarının başına gelebilecek her türlü tehdit ve tehlikeyi eğer önceden öngörüp önlem alabiliyor isek buna da biz bilgi güvenliği diyoruz. Tabii ki bunu kişisel verilerimizin güvenliği olarak ifade edeceksek bir kişinin başına gelebilecek her türlü tehdit ve tehlikeyi, özel hayatıyla, mahremiyetiyle ilgili, verileriyle ilgili, önceden öngörüp tedbir alabiliyor isek bunu da kişisel verilerin güvenliği olarak ifade edebiliriz. Burada, değer de çok önemli tabii ki. Bakın, bir cep telefonunu bilmenin değeri ne olabilir, bunu da sorgulamamız gerekiyor çünkü değerle koruma seviyesi de doğru orantılı durumlar.

Şimdi, bilgi güvenliğine temel olarak baktığımızda dört ana unsur var bilginin elektronik ortamlarda güvenliğinin sağlanması için. Bunları mutlaka anlatmış olabilir arkadaşlarımız ama ben üzerinden hızlıca geçeyim. İşte, bilginin bir noktadan diğer noktaya, verinin bir noktadan diğer noktaya taşınması esnasında eğer üçüncü taraflar o veriye erişebiliyor ise burada bir ihlal var. Biz bunun önlenmesine yönelik olarak yapılan çalışmalara gizlilik diyoruz. Eğer, veri değiştiriliyor ise bir noktadan diğer noktaya aktarılırken, bu değişimin olup olmadığını belirlemeye biz bütünlük diyoruz ama elektronik ortamları "kara ortamlar" olarak ifade ediyoruz. Bu ortamlarda gönderenin ve alanın kimliklerinin belirli olması gerekiyor. Buna "kimlik doğrulama" diyoruz ve alanın aldığını, gönderenin de gönderdiğini inkâr edemediği ortamlarda da bilginin inkâr edilememesi -alanların gönderenlerin- bunun sağlanmasını da "inkâr edememenin sağlanması" olarak ifade ediyoruz. Bunun arkasında da şifreleme bilimi var. Bu şifreleme bilimi ile bu söylediklerimiz gerçekleşebilir. Gizlilik için şifreleme algoritmaları kullanıyoruz, bütünlük için özetleme algoritmaları, kimlik doğrulama için elektronik imza -5070 sayılı Kanun'umuzda ifade edilen- ve inkâr edememe için de elektronik imza altyapısı sunan açık anahtar altyapısı ve sertifika sağlayıcıların sunduğu hizmet olarak bakıyoruz. Ama buna ilave olarak kayıt tutma, buna ilave olarak emniyet tedbirleri alma gibi, giriş kontrolleri sağlama gibi unsurlar da bu ana bilgi güvenliğini sağlayan veya destekleyen unsurlar olarak karşımıza çıkıyor.

Şimdi, temel olarak baktığımızda bilgi güvenliğine, aslında, burada, resimde gördüğünüzde, kişiler ve cihazlar haberleşiyor. Kişiler cihazlar üzerinden haberleşiyor, bilgi cihazlar üzerinden haberleştiğinde bir ağ var, ağın güvenliği, ağ üzerinden bilgi aktarılırken kablolu kablosuz bir ortamın güvenliği ve bir de kullanılan cihazların yayınım güvenliği gibi pek çok unsurlar olabilir. Bu temel olarak sunulan bir güvenlik bakış açısı ama günümüze geldiğimizde, bakın, ilk 6 tanesi bilinen, çok iyi bilinen unsurlar ama kullandığımız donanımdan yazılımına, işletim sisteminden sosyal ağlara, mobil cihaz güvenliğinden… Yani bakıyorum, pek çok milletvekilim akıllı telefon kullanıyor ama kullanmayanları da gördüm. Bunların güvenliği, web teknolojileri güvenliği, uygulamaları güvenliği, protokol güvenliği, sunucu güvenliği… Bakın, biz bu teknolojileri konuşuyoruz, IPv6 güvenliği, yeni nesil İnternet teknolojilerinin güvenliği. Artık her bir kullanılan cihaza bir numara verilmesi ve bunlarla

iletişim. Ülkemizde de bununla ilgili bir projede çalıştığım için söyleyebilirim, bu konuda bile bir güvenlik açığı var. Bunlar üzerinde çalıştık, bir altyapı oluşturduk. Şu anda ULAKBİM'de tüm sektörün ve araştırmacıların kullanabileceği bir altyapı var. Burada deneme testleri yapabilirler.

Bakın, siber güvenlik diyoruz, hâlâ şifre güvenliğinden bahsediyoruz. Neden bahsediyoruz? Yapılan istatistikler maalesef şifrelerimize önem vermediğimizi hâlâ gösteriyor kendi üniversitemizde bile. Ben aynı zamanda Bilgi İşlem Daire Başkanlığına da bakıyorum. Maalesef hocalarım bu konuda biraz dikkatsizler uyarmamıza rağmen. İşte, güvenli yazılım geliştirme teknikleri, steganografik güvenlik, RFID güvenliği, bakın bunlar, kritik altyapı güvenliği gibi… Google güvenliğini bile gündeme alacağız. Bugün size Google'ı farklı bir bakıştan anlatacağım. Bu ortamlarda ihlaller nasıl olabilir, bunu hep beraber, belki, değerlendirme imkânımız olacak. Bunu uzatabiliriz. Eminim sizlerin de burada benim bilmediğim pek çok öneriyi yapabileceğinizi düşünüyorum.

Şimdi, bilgi güvenliğinin kapsamına baktığımızda -şimdi, biraz önce bilgiyi tanımladık veri, bilgi, öz bilgi dedik- bunun, verinin üretildiği andan artık insanın doğumundan ölümüne kadar olan süreç olduğu gibi, bilginin de doğduğu andan ölümüne kadarki tüm süreçleri eğer biliyor isek biz bilginin güvende olduğunu düşünüyoruz. İşte, üretildiği andan erişimine, işlenmesine, depolanmasına, aktarılmasına, yok edilmesine kadarki süreç… Türkiye yok edilmeyi Ankara Emniyet Müdürlüğünün "Bilgisayarları artık yakacağım" dediğinde, harddiskleri yaktığında öğrendi genel olarak basına düştüğü için. Çünkü bunlardan bilgilerin alınabileceğini biliyoruz. Kırıkkale'ye gittiğimizde, ya, ben de oradan pek çok harddisk satın aldım. Biz motorların… İlk önce ben mobil robotlar üzerine çalıştım ama robotlar için inanın kiloyla harddisk satın aldığımızı biliyorum. İçinde müthiş bilgiler vardı. Bakın, bunlar dışarıya satılabilen… Eğer bu aşamaları bilmiyor isek biz güvenlikten bahsedemiyoruz.

Şimdi, "Bilgi sahibine veya sahip olana hizmet eder"i mutlaka farkında olarak ne yapmamız gerekiyor? Hayatımıza yerleştirmemiz gerekiyor kişisel verilerimizi koruma adına.

Şimdi, bilgi güvenliği sağlandığı ölçüde artık güç. Bilgi güçtür demiyoruz, güvensiz ise bilgi güç değil artık. Çok da tehlikeli, başınıza da zarar açabiliyor. Ama burada önemli olan bir husus da bilginin mutlaka üretilmesi gerektiği yani üreten ancak değerinin farkında, üretmediğimizde bilginin çok farkında olamıyoruz.

Şimdi, "Matematiksel olarak bilgi güvenliği nedir?" dediğimizde aslında bilgi güvenliği… Siz yüzde 99,9 koruma tedbirlerini alın, teknolojik alın, insan alın, fiziksel alın, biraz önce bahsettiğimiz tüm unsurları alın ama binde 1 bir korunmasızlık, binde 1 ihlal eşittir yüzde 100 güvensizlik. Ya, artık yüzde 100 güvenlik olmadığını bilerek bu işi yapmak gerekiyor. Tabii, ki buna kişisel verilerin mahremiyeti olarak baktığımızda da yüzde 100, işte, kişisel gizlilik ve mahremiyetin ihlali olarak da ifade edebilirsiniz. Çünkü bir kişi çok küçük bir olaydan dolayı ne yapabiliyor? Pek çok farklı şekilde de zarar görebiliyor.

Evet, İnternet'te…

ŞUAY ALPAY (Elâzığ) – Affedersiniz.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Buyurun.

ŞUAY ALPAY (Elâzığ) – Binde 1 korumasızlık eşittir yüzde 100 güvensizlik.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Güvensizlik, tabii ki, evet, çok sert ama… Bu zihinlerde kalsın diye söylüyoruz çünkü bakın, bütün tedbirleri alıyorsunuz, bir unsuru atladığınız anda ifşa oldunuz, bu eşittir güvensizlik.

ŞUAY ALPAY (Elâzığ) – Bir de, yalnız "Yüzde 100 güvenlik yoktur." deyince aslında iş biraz bilimsel olarak da bitmiş olmuyor mu? Şimdi, binde 1'i de konuşmanın çok fazla manası yok o zaman, yüzde 100 güvenlik yoksa.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Evet, şimdi, yüzde 100 güvenlik yoktur, doğrudur. Ben de güvenlik derslerinde bunları… "Madem Hocam, güvenlik yok ise biz niye güvenlik dersi alıyoruz." diyor öğrenciler.Tabii ki amaç burada "güvenlik yoktur"u vurgulamak için… Bunun tedbirini almak, matematiksel olarak yüksek maliyet gerektiriyor. Yüzde 100 biz de onu sağlayamayacağımıza göre yoktur ama bu riskler minimize edilebilir. Bunu ifade etmek için söyledim.

Bakın, İnternet ilk kurulduğunda sadece askerî bir projeydi, bugün İnternetimiz böyle, gelecekte bu ağ yapısını bütün dünya farklı şekilde daha karmaşık hâle getirecek. IPv6'ya geçtiğimizde artık bu "network"lerden milyonlarcası karşımızda olacak. Evet, bunu sadece bir dikkat çekmek için söyledim.

Şimdi, isterseniz kötü haberle başlayalım. Bilgi çağında korkularımız neler? Artık kapsamlı ve planlı saldırılar sürekli artıyor. Bakın, gerçekten yüksek para ödeniyor, yüksek emek harcanıyor ama saldırılara bakıyorsunuz, planlı ve kapsamlı saldırılar her zaman yine bizlerin gündeminde. Ama bu kötü haberimizdi, daha kötüsü var: Daha kötü haberimiz de saldırganların ihtiyaç duyduğu araçlar artık İnternet'ten çok kısa sürede elde edilebiliyor. İnanın, sizler de üç dakika içerisinde bir saldırgan olabilirsiniz. Yani bir yazılımı indirip bir sisteme saldırıp o sistemin açıklarını elde edebilirsiniz veya birkaç konu biliyor isek bir araştırma yaparak sistemin açıklarını öğrenip oraya saldırı yapabilirsiniz. Mesela Google örneğini biraz sonra size anlatacağım.

Evet, şimdi, durum bu ve böyle de olunca artık saldırganlar veya saldırgan eğilimli veya bu işi sadece hobi veya merak için yapanlar da ne yapıyor? İnternet'te saldırgan hâline gelebiliyor.

Evet, artık, günümüzde de baktığımızda bu grafik gittikçe artma eğiliminde. Kapsamlı, planlı, daha önceden oynanmış senaryolar ne yapılıyor? Gündeme getiriliyor. Bunu devletler yapıyor, mesela "stagnet" örneği gibi, bunu kendini farklı kimliklere büründüren gruplar, terörist gruplar yapabiliyor veya çıkar amaçlı gruplar yapabiliyor veya istihbarat amaçlı veya arkasında pek çok şey olabilir.

Şimdi, saldırıları iyi anlamak gerekiyor. Saldırılar aynen bir gauss dağılımı gibi, bir saldırı, bir ihlal olduğu zaman aslında bunu eğimin başlangıcı gibi düşünebilirsiniz, en tehlikeli an bu an çünkü -kimse bilmiyor- sistemlere erişip oradan veri alabilirsiniz ama duyulmaya başladı mı pik yapıyor, pikten sonra artık herkes bildiği için çözüm geliştiriliyor, çözümden sonra eğri kaybolmaya başlıyor, tabii ki önleminizi almışsanız. Önlem alınmamış ise ne oluyor? Çözüm çok karşımıza çıkmıyor. Burada taralı alan en kritik zaman. İşte, burada sistemlere daha çok saldırıların yapıldığını tespit ediyor. Bu dağılımı bilirsek ona göre hızlı çözüm ne yapabiliriz? Sağlamış olabiliriz.

Şimdi, bilgi çağı diyoruz, aslında bilgi çağında saldırıları şöyle gruplandırıyoruz: Saldırgan, hedef, yol, kasıt ve araç olarak. Şimdi, saldırganlar artık -eskiden tekti- şu anda takım çalışıyorlar. İnanın iyi insanların yapmadığını, kötü insanlar birlikte neler başarıyorlar elektronik ortamda, bazen çok şaşırdığımı, hayretler içerisinde kaldığımı burada ifade edebilirim.

Hedef olarak baktığımızda, artık hedefler, kişiler -doğrudur- kurumlar, ülkeler ve artık çıkar amaçlı ne elde etmek istiyorsa vurmak istediği hedefe yöneliyor. İşte, burada çok hedefli saldırı ve ağ saldırısı da popüler hedefler arasında. Şimdi, yola bakıyorsunuz, kullanılan metoda, doğrudan saldırılar eskidendi, şimdi dolaylı saldırıyorlar. Bir kişiyi direkt hedef almıyor. Dolaylı olarak farklı gruplar üzerinde ne yapıyor? Bu saldırılarını yapıyor.

Kasıtlar: İşte bu, bilgi hırsızlığından tutun, kaynak yıkımına, ön saldırılardan sistem aksattırma saldırılarına kadar pek çok saldırı olabiliyor. Araç olarak baktığımızda da, eskiden yerel araçlar vardı, bilgisayarınıza yükleyip saldırmak durumundaydınız. Şimdi uzaktan araçlarla bile bunu yapabiliyorsunuz.

Şimdi kısaca birkaç istatistikten bahsetmek istiyorum: Mesela, yapılan saldırıların yüzde 70'i uygulama seviyesinde yani insanların geliştirdiği yazılımlardan kaynaklanıyor. Mesela, ticari içerikli web sayfalarının yüzde 75'inin korunmasız olduğunu istatistikler söylüyor. Web uygulama yazılımcılarının yüzde 60'ının güvenli yazılım geliştirme tekniklerini bilmediği söyleniyor. Bizdeki üniversitelere ben bakıyorum, güvenli yazılım geliştirmeyle ilgili henüz bir dersimiz yok; kitapları var, kaynakları var. Bunu uygulayan kurumların sayısı da çok az ülkemizde.

Şimdi, saldırılara temel olarak bakıldığında, aslında saldırıların yüzde 20'sinin teknolojiden kaynaklandığını yani teknoloji tabanlı zafiyetlerden kaynaklandığını ama yüzde 80'i insanın içerisinde bulunduğu, insanın geliştirdiği… Hoş, teknolojiyi de öyle düşünebiliriz ama insandan kaynaklandığını ifade ediyor. Mesela, İnternet'e eriştiğimiz HTTP protokolünün de güvenlik camiasında adı "Güvenli sistemlere güvenli erişim protokolü." Burada saldırgan gözüyle söylüyorum bunu: Bir saldırganın sisteme kolaylıkla erişebileceği bir ortam, bir yol olarak bakıyorlar.

Pekâlâ, bilgi her yerde diyoruz bilgi çağımızda, zamandan, mekândan bağımsız, artık, bilgi bir güç, dedik. Bilgi ekonomisi konusu önemli veya burada alınan her kararın bilgi ekonomisini etkileyeceğinin -burada özellikle kırmızıyla belirttim- farkında olmamız gerekiyor ve kapasiteler de

sürekli artıyor. İşte, big data kavramları gündemde. Dünya bunu tartışıyor, bunlardan neler elde edilebilir, buna bakıyor ve burada kişisel verilerin ihlali konusunda neler yapılabilir… Bunun üzerinde çalışmalar artık ülkemizde de yapılmaya başlandı. Bir operatörden geçen hafta bir mesaj aldım. "Sizinle ilgili, veri tabanlarında araştırma yapıp size özeli tarife sunmamızı ister misiniz?" diyor. Bunun anlamı şu: Araştırıyor, arka planda, izin vermemi istiyor yani operatörde bu farkındalığın başladığını ben görüyorum orada ama başka yönden çok dikkat etmiyor olabilirler ama böyle bir farkındalık başladı. Artık bilgi çağında savaşlar içerisindeyiz, bilgi yaygınlaşıyor dedik. Mobil ortamlar artmaya başladı ve artık İnternet'ten daha fazla telefon kullanıcısı var dünyada ve ülkemizde de son bir-iki yıl içerisinde mobil kullanıcı, özellikle İnternet tabanlı erişimde mobil erişime baktığınızda müthiş artış var ama burada bir savaş olduğunun lütfen hepimiz farkında olalım. İyilerle kötülerin arasında amansız bir savaş var. Şimdi, neden oluyor bu dediğimizde bakıyoruz kötücül kodlar yani bu zararlı yazılımlar daha çok burada etken çünkü milyarın üzerinde zararlı yazılım var, pek çoğu da gerçekten daha çözemediğimiz yazılım türleri. İşte, Stacnet üzerinde o kadar çok çalışma var ki hâlâ anlamış değiliz arkasında devlet mi var, birimler mi var, ne var? Ama yapılan çalışmadan o işin büyüklüğünü görüyorsunuz. Eğitimsizliğin yattığını düşünüyoruz, insan faktörü burada en önemli adım ama burada süreçlerin yönetilememesi de en büyük sıkıntı. İşte biraz önce "İyilerle kötülerin aslında amansız bir savaşı var." dedik. Burada literatüre baktığımızda saldıran taraf ve savunan taraf diye ikiye ayrılıyor. Aslında bilinen savunma ve saldırı teknikleri ama habersiz ve tarafsız bir tarafımız var bizim. Biz ne saldırganız ne savunuyoruz ama tabii ki bu habersiz tarafın aslında saldırgan tarafta yer aldığını da burada belirtmekte fayda var. Çünkü günümüz teknolojileri ne yapıyor? Saldırganlar, habersiz olan kitleleri de saldırgan hâline getiriyor, onun teknolojilerini kullanarak gruplar, Hotnet'ler oluşturup ne yapıyor? Onların cihazları üzerinden farklı ortamlara saldırı yapabiliyor. Belki en tehlikelisi de bu. Mutlaka bir taraf olmamız gerekiyor.

Şimdi, saldıran tarafa bakıyoruz, bunlar gerçekten donanımlı arkadaşlar, biraz önce dediğimiz gibi, kendilerini geliştiriyorlar, iyi iş birliği yapıyorlar, bilgi seviyelerini artırdıkları gibi takımlarını da geliştiriyorlar, hedefe kilitlenip gerçekten hedefine, başarıya ulaşmada önemli adım atıyorlar. Tabii, bununla ilgili olarak da kötücül kodlar gibi yazılım veya yazılım platformlarındaki açıklardan faydalanarak bunları yapıyorlar ve örgütleniyorlar ve maalesef iyilerden önde gittiklerini burada söylemekte fayda var ve habersizleri de, tarafsızları da kullanıyorlar. Şimdi, savunan tarafa baktığımızda en zayıf halka çünkü bilgisizlik, ilgisizlik, hafife alma had safhada burada gördüğümüz. Tabii, bunun arkasında korunma maliyetleri olabilir, bunun arkasında zaman ayıramama olabilir, bunun arkasında pek çok gerekçe olabilir ama daha çok yatırım ve eğitim eksikliğinin burada olduğunu görüyoruz. Savunan tarafta yine, elektronik dünyanın doğasında olan bir güvensizlik var.

Şimdi, bilgi çağındaki savaşlara şöyle bir baktığımızda artık gerçekten kapsamlı dedik, bizler de burada kapsamlı çalışma yapmalıyız yani savunan taraflar olarak. Çoklu saldırılar, popüler,

bunlar, senaryosu yazılmış, denenmiş oluyor, karma yapılar içeriyor. Karma yapılar derken, yazılım, donanım ve insan faktörleri ve günlük hayatımızda kullandığımız pek çok veya içinde bulunduğumuz zaafiyetleri de kullanarak -ne yapılıyor-sistemlere erişilebiliyor. Ve bilinmeyenleri ve düşünülmeyenleri düşündükleri için de gerçekten ilerideler. Tabii, bunlar takip gerektiriyor, bunların yaptığı işleri bilmek gerekiyor, karşı önlem almak gerekiyor ve yüksek bilgi birikimiyle çalışıyorlar gece gündüz. İyiler biraz rahat bu konuda.

Şimdi, casus yazılımlara bakıyoruz. Bakın, mobil cihazlar üzerinde yaptığım bir araştırmada sadece android üzerinde 5 bin yazılım var, bu kişisel verileri ihlal edebilecek 5 bin yazılım var, uygulama var, -yazılım demeyeyim de- uygulaması var. Bugün, iPhone tarafına baktığımızda da bunların sayısı da, işte, -android arkadan geliyor- 500 binin üzerinde uygulaması var şu anda iPhone'nin. Yani, içerisinde olabilecek ihlalleri söylemeye herhâlde gerek yok diye düşünüyorum.

Bunlar, casus yazılımlar ne yapıyor? Bakın, "Sayıları artıyor." dedik. 2011'de sadece 100 bin yeni virüs ve casus yazılım çıktı, bunların da pek çoğunun da çözümü olmadığı ifade edilmişti. 2012'de bu sayıların düşmesi beklenirken bu sayı giderek artıyor çünkü teknoloji kullanımı yaygınlaşıyor, uygulamalar gelişiyor. Geliştikçe, tabii, ilgi artınca da zafiyetler de maalesef artıyor. Bu casus yazılımlar kendilerini saklayabiliyorlar, görünmez olabiliyorlar. Silseniz bile tekrar kendisini kopyalıyor, işte, solucan mantığında çalışan yazılımlar olabiliyor. Belirli bir süre var oluyor, sonra kendilerini silebiliyorlar. Tabii ki o varoluş şeyi sadece sizin şifrenizi elde ettikten sonra kendisini silen yazılımlar var. Bunları alıyor, başka yerlere mail atabiliyor, sms atabiliyor. Size bunların demolarını burada yapabilirdim ama yapıldığını basından öğrendiğim için çok gerek görmedik ama ihtiyaç olursa onu da gösterebilirim.

Şimdi bakıyoruz, siber savaş gündemde. Casusluktan tutun da manipülasyona, propagandadan tutun da dolandırıcılığa kadar, sistemleri devre dışı bırakmaya kadar pek çok unsur yine gündemde. Şimdi, silahlara bakıyoruz, bu elektronik kurtçuklar, biraz önce dediğimiz virüsler bizim siber silahlarımız. Yani, milyar dolar verip alamayacağınız silahlar yerine İnternet'ten indirip kullanabileceğiniz, ücretsiz hâle dönüşebilecek silahlar hâline geliyor. İşte, hizmetin engellenmesinden tutun da virüslere, klavye izleme yazılımlarından tutun da köstebek veya casus yazılımlara, yemlemeden işte istem dışı elektronik posta veya ağ trafiği dinlenmesi gibi bizim pek çok siber silahımız olabiliyor.

Evet, şimdi, Afganistan'da yaşandığı için hafıza kartları en modern silah olarak ifade ediliyor. Neden? NATO tesislerine giremeyen saldırganlar, teröristler ne yapıyor? Hafıza kartlarıyla giriyorlar sistemlere. Nasıl mı? Pazarda satılan bir hafıza kartının -memory stick'in- içerisine casus yazılım yükleyerek öyle sattırıyorlar. Ucuza sattırıyorlar, oradan ihtiyacı olan da gidiyor, alıyor ve oradan sistemlere erişebiliyorlar yani sistem böyle zafiyetleri kullanıyor. Birisini düşürerek bir bankanın sistemine girdiğini biliyoruz, literatürde öyle örnekler var. Birisi yürürken kasti olarak memory stick'ini düşürüyor, arkasında yönetici geldiğini görüyor; yönetici de alıyor, -meraklı insanlar, bu ITC'ler

meraklı oluyor- "Yahu bunda ne olabilir?" diye taktığında bilgisayarına, işte, casus yazılım iniyor ve ondan sonra gerekeni yapıyorlar. Yani bu böyle bir olay. Bakın, çok, işte binde 1 dediğimiz, biraz önce sorduğunuz binde 1'lik zafiyet bu demek, tüm sistemleri açık hâle getiriyor. Dalgınlık, merak, -işte insanız- bu tür unsurlar çok gündemde. Tabii ki burada amaçlar sisteme etkisiz erişimler, sistemin bozulması, hizmetin engellenmesi, -tabii ki biraz önce de bahsettiğimiz- verilerin değiştirilmesinden tutun da yok edilmesine, ifşa edilmesine, çalınmasına kadar pek çok unsurları içeriyor.

Şimdi, WikiLeaks'i buraya özellikle koydum. WikiLeaks dünya için çok önemli bir örnek, üzerinde tartışılması gereken bir örnek. Belki bunu ülkelerin kişisel verilerin ihlaline farklı bakış açısı kazandıracak da bir örnek olarak gördüğüm için burada ifade etmek istiyorum. Güvenlik açısından iyi dersler çıkaracağımız bir örnek olarak buna bakıyorum. Bir sanal savaş denemesi bu, farkındayız veya değiliz, bu kişisel yorumumum benim, kendisini ve diğer ülkeleri nasıl etkileyecek, bunu gördüklerini düşünüyorum. Yani böyle bir denemenin arkasında ne olabilir, ülkeler nasıl reaksiyon gösterebilir, bunu denediler. Mesela, daha önce Orta Doğu'ya Cezayir yakınlarında geçen kabloyu kestiler, "Gemi geçerken sürtündü ve fiber kesildi." dediler. Orada bir deneme yaptılar mesela. Şimdi de böyle farklı denemeler yapıyorlar. Dünyaya bu açıdan bakmamız gerektiği için bu örnekleri paylaşıyorum. Geliştirilen teknolojilerini test ettiler. İşte, Facebook, Twitter, diğer şeyler bize ne kadar destek oluyor böyle bir operasyonda, bunları test ettiler. Facebook'un arkasında farklı Plug-in'lerle destek verdiklerini basından sizler de mutlaka okumuşsunuzdur. İnternet ne kadar kontrol edilebiliyor, edilemez, bunu da gördüler aslında arka tarafta ülkeler. Bir defa, İnternet'i kontrol ediyorlar, ondan emin olalım da ama diğerleri tarafında bu işle nasıl gidiyor, biraz onun da büyük resmini çıkardıklarını düşünüyorum ve farklı ülkelere de farklı mesajlar verdiler. Her ülkenin bundan ders çıkardığını düşünüyorum.

Şimdi, Google'a gelelim. Burada Google kullanmayan var mı içimizde? Google'ı lütfen isim olarak algılamayalım, sadece bir arama motoru olarak bakalım. Ben de kendi bakış açımdan Google'ı size bugün farklı şekilde anlatacağım. Gerçekten işleri mükemmel yapan, ücretsiz yapan böyle bir hizmet, dünyada herhâlde başka bir hizmet yoktur diye düşünüyorum. Mükemmel bir arama motoru gerçekten ve en çok tercih edilen arama motoru. İşte, bunun farkına vardığı için Ruslar da Yandex'i şu anda bizde reklamlarla geliştirmeye çalışıyorlar. Mükemmel de hizmet veriyor gerçekten, ben bir akademisyen olarak çok mutluyum hizmetinden. Artık, pek çok şeye kolayca erişebiliyorum. En son çıkan yayınları hızlıca takip edebiliyorum. Sadece bu akademikler için değil, kitaplardan tutun çeviri sistemlerine kadar… Çeviriyi kullanmayan var mı içimizde? Ama en iyi kullanan da saldırganlar. İnanın, öğrencilerimden gördüğüm için… Bir gün öğrencim dedi ki: "Hocam, bir Çin sitesini çökerttim." "Nasıl yaptın? Çinceyi ne zaman öğrendin?" dedim. "Hocam, Google var, çeviriyle yaptım." dedi. Tersi de var, onlar da çevirerek saldırı yapıyor. Evet, şimdi, bizim bilmediğimiz çok özellikler var. Değeri bunu hazırladığımda 200 milyar dolardı ama şu anda trilyonlara yaklaştığını söyleyebiliriz. Şimdi, Google'ı belki hatırlamazsınız ama Google'ın ilk çıkan web sayfası bu, ben bunu

ilk gördüğüm günü hatırlıyorum. Çok da etkilenmediğimi söyleyeyim size ama bugün geldiği noktayı o gün görememiştim şahsen, bilmiyorum gören var mı? Geldiği nokta inanılmaz. Şimdi, verdiği hizmetlere bakıyorsunuz, AdSense'den tutun AdWords'e, akademikten Analytics'e... Yani, bir web sayfanız var, buraya kimler girmiş çıkmış, ne zaman girmiş çıkmış, hangi ülkeden; bunların istatistiklerini veren ücretsiz altyapılar sunuyor. Uygulamaları var, son çıkan teknolojilerini tanıtıyorlar. Şimdi, blog gibi şeyler belki biliniyor ama yazılan kodlar içinde Google kodu var, kitapları var, patentleri var, makaleleri var. Bunları ücretsiz sunabilen yapıları -ne yapıyor- bizlere sunuyor. Şimdi, bakıyorsunuz, haritadan tutun da burada pek çok hizmetleri var. Ha, bu hizmetleri farklı şekilde değerlendireceğiz ama burada bir şeye dikkatinizi çekmek istiyorum: Google'ın sahip olduğu sunucu sayısına lütfen bir bakın, 1 milyonun üzerinde sunucusu olduğunu ifade edelim. Bakın, dünyada milyon üzerinde arama motoru var ama Google'ın sahip olduğu sadece sunucu 1 milyonun üzerinde. Ya, ne kadar büyük bir veriyle uğraştığımızın farkında olalım. Onların bir iddiası var, gerçekten okuduğumda çok etkilenmiştim: "Biz bir kelimeyi bile israf etmiyoruz." diyorlar. Buradan nasıl bir anlam çıkartırsanız, artık onu size bırakıyorum. Beni gerçekten üç gün böyle çok etkilemiş, daha sonra da bu konulara onun için merak saldım, bu konularda çalışmaya başladım.

Şimdi, isterseniz bu hizmetleri farklı bir açıdan değerlendirelim. Google akademi var, bilimsel çalışmalarımız. Şimdi, Google'dan önce de başka... Geçen hafta Elsevier'den geldiler, Elsevier'de ben, ülkemizde hangi alanda, hangi bilim insanlarının 1 numarada olduğunu ben biliyorum. Gazinin en değerli bilim insanının kim olduğunu biliyorum. Nereden öğrendim? Elsevier'in veri tabanından. Hangi konuda dünyada ilklere oynuyor, bunu biliyorum. Hangi araştırma grubu önemli çalışmalar yapıyor, biliyorum. Üç dakikada öğreniyoruz bunu. Ve ellerinde müthiş bir veri tabanı var. Daha önce de Thomson Reuters'in veri tabanlarına baktım, inanın kendimi orada farklı gördüm. Geldiler, Thomson Reuters girdi verileri, inceledi ve bana önerilerde bulundu. "Hocam, yanlış dergilerde yayın yapıyorsunuz." dedi mesela. İlk kez bunu onlardan duydum. "Çünkü yayın kalitesi yüksek ama siz kalitesi düşük dergiye yayın göndermişsiniz." diyor, bunu söylüyor bana, benim haberim yok. Big data dediğimiz bu. Gerçekten bunu dahi, bu hizmeti de veriyorlar. Girin, bakın. Yani, kişileri de böyle değerlendirdiklerini düşünün. Kişinin kendinin farkında olmadığı pek çok verisini kişinin yüzüne söyleyebilecek altyapılar var şu anda. Ya, ben de kendime farklı gözle artık yeni hedefler çizmek durumunda kaldım, "Keşke bunu daha önce bilseydim." dedim.

ŞUAY ALPAY (Elâzığ) – Köye dönüş hazırlıklarına başlayabiliriz.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Yok, yok, bunu korkutmak için değil, bunları kullanmamız da gerekiyor. Bakın, burada değerlerimizin farkında olalım, kendimizi, hangi konuda zayıfsak o yönde de geliştirelim. Mesela, Google Docs var, oluşturulan dokümanları tutuyor, size sunuyor. Bakın, Gmail, kimlerle yazışıyorsunuz? Size soralım: Bir ticaret şirketiniz olsa, ücretsiz -burada daha önce tanıştığımız

vekillerimiz var, ticaretle uğraştığını bildiğimiz- bu hizmeti verir misiniz? Ama bunlar veriyor, arkasında da tabii ki bu verileri değerlendiriyorlar. Bizi nasıl değerlendiriyor? İnanın silmeyin dedikleri o Gmail'den, benim nasıl bir akademisyen olduğumu, nasıl bir kişi olduğumu, neleri sevdiğimi, neleri sevmediğimi, kimlerle haberleştiğimin analizini yapıyorlar ve bunu birkaç dakika içerisinde yapıyor. Kişisel olarak önemli değil ama ülkenin durumunu bizden iyi biliyorlar. Bakın, esas tehlikeli kısım bu. Ülke paranoyak mı, değil mi? Ülke sağlıklı mı, değil mi? Ülkenin gidişatı nasıl? Eğitimli mi, değil mi? Aranılan kelimelerin istatistiklerinden bunu biliyorlar ama biz bunun farkında değiliz ama onlar bunu çok net biliyor. Ona göre strateji geliştiriyorlar ve bunları ilgili birimlere de satıyorlar, artık bu bir ticaret. Evet, Gtalk diyoruz, kimlerle konuştuğumuzu biliyorlar. Bakıyoruz bloglar, kimlerle yazışıyorsunuz bunları biliyor, ne yazıyorsunuz. Google Earth'ı var, bağlantılarımızı biliyorlar, network'ümüzde kimler var; Wallet var, finansal durumumuzu biliyorlar; Picasa var, resimlerimizi… Şimdi, Google'ın hizmeti var biliyorsunuz, resim içerisinde resim araması bile yapabiliyor artık İnternet'te, sesimizi bile arayabiliyor. Bakın, ses araması yapabilen servisleri var. İşte, Google Reader'la neyi, kimi takip ediyorsunuz, bunun farkındalar. Bakın, büyük tabloyu koyunca gerçekten -biraz önce sayın vekilimin dediği gibi- insan köye dönüş hazırlıklarını yapalım gibi düşünebiliyor.

YILMAZ TUNÇ (Bartın) – Köylerde de ADSL var artık Hocam, dönse ne olacak.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Şimdi, yok, bunlarla mücadele edecek yerler de herhâlde burası yani bunu ülkede çözecek birimler de burası. Bizde üniversiteler, işte, araştırma yapıp bunları -ne yapacağız-işleyip… Arşiv hizmeti var, verileriniz nedir, bunları biliyor. İşte, Google'a bu gözle bakmak gerekiyor. Google bizi bizden iyi tanıyor, analiz ediyorlar. Hani biraz önce dediğim "Bir kelimeyi bile israf etmiyoruz." diyor, gerçekten öyle yapıyorlar. Bunların çok farklı bilgi birikimi, deneyim elde ettiklerini söyleyebiliriz. Yalnız burada lütfen Google ismini kullanmayalım, bütün arama motorları bunu yapıyor. Ben örnek olsun diye bunu sizlere aktardım. Çünkü sanki Google casusluk yapıyor, bilmem ne yapıyor gibi şeyleri söylemeyelim. Arama motorları olarak, eğer basından arkadaşlarımız varsa lütfen öyle yazsınlar. Google'ı hedef göstermek değil ama işini iyi yapıyor. İstemiyorsan kullanma.

Pekâlâ, arama motorlarına baktığımızda, şimdi, kişisel, kurumsal ve ulusal bilgilere erişim için en güzel ortamlar artık, açık olan bilgilere erişim. Kapalı olduğunu düşündüğümüz bilgilere de erişim yapıyorlar. Gizli olan bilgilere de erişiyorlar. Özel hayatı ilgilendiren verilere de kısmi de olsa erişiliyor. Biz farkında değiliz ama birleştirince pek çok şey anlam ifade edebiliyor. Bir veri oradan, bir veri oradan, bir veri oradan… Bunu otomatik yapan yazılımlar var ve bunu istihbarat servisleri de kullanıyor mesela ama burada istihbarat servisleri uluslararası kullanıyorlar yani esas tehlikeler bunlar.

ERDAL AKSÜNGER (İzmir) – DPI programı…

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Efendim?

ERDAL AKSÜNGER (İzmir) – DPI'ler mi?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Evet, açık istihbarat içinde en iyi ortam. Yani, bir kişi geldi mi ne yapıyoruz? Hemen İnternet'ten ona bakabiliyoruz, kişisel olarak bakıyoruz ama pek çok şey için de bu ortamlar kullanılabilir. Tabii ki bu dünyanın en iyi casus yazılım sistemi var Google'ın üzerinde ve dünyanın bilgisini topluyorlar, işliyorlar ve bunu değerlendiriyorlar ve ülkesine, ülkelerine hizmet eden en iyi ortamı da sunuyorlar. Bizi bizden iyi tanıyorlar, ülkeleri ülkelerden daha iyi tanıyorlar, daha iyi analiz ediyorlar. Kelime, cümle, resim ve ses araması yaptırabildiğini söyledik. Mesela, encrypted.google.com var. Eğer siz aramalarınızda şifreli haberleşmek istiyor iseniz böyle bir servis de sunuyor bakın. Eğer benim haberleşmemi kimse bilmesin, ne aradığımı bilmesin diyorsanız encrypted servisi var. Yani şifreli haberleşme arama yaptırabiliyorsunuz. Şimdi, burada arama yaparken bile fazladan hiç bir kelime yazmamalıyız. Birincisi enerji harcamasını önleme adına, ikincisi de bizimle ilgili bilgilerin gitmesi adına. Aradığınız kelime sizi ele veriyor. Nelere baktığınız, nelerle ilgilendiğiniz. Bir de ülkenin haritasının çıkarıldığını düşünün. Tıkladığınız yerden lokasyonunuzu biliyorlar. Bu servisler öyle servisler.

ŞUAY ALPAY (Elâzığ) – Peki Hocam, şifreleri yaparak hizmet veriyor ama sonuçta onun üzerine yaptığı için onun da bir manası yok, onlar açısından bir bilinmezlik değil.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Tabii, tabii, doğru; başkaları açısından, çok doğru.

Şimdi, LAS'in bir kuralı var: Kırılamayan hiçbir yazılım dışarıya satmıyorlar veya satıyor ise Amerika içerisinde farklı, Amerika dışında farklı çalışıyor. Bize sundukları servislerin şifreleme seviyesi düşüktür. Yani onu söyleyelim, ülkenin öyle bir kuralı var. İşte, güvenlik açığı oluşturabilecek hususları kapatıyorlar. Şimdi, ben hack'lemeyle ilgili bazı şeyleri araştırıyorum. "Çok fazla kişisel verilerle uğraşıyorsunuz, kısa bir süre size hizmet veremeyeceğiz." diye kapatıyor. İlk kez gördüm ben de bakın. Bu kadar detay, benim ne araştırdığımın bile farkında. Arkada kullandığı teknolojiler; derin, dehşet teknoloji kullandıklarını söyleyebilirim. Ya, uyarıyor "kişisel veriyi ihlal ediyorsunuz" diyor bakın. Saldırı falan yapmıyorum, sadece İnternet'te arama yapıyorum, biraz sonra da size o aramalardan bazılarını göstereceğim. "Ama burada ihlal edici arama yapıyorsunuz." diye uyarıyor. Demek ki bunun anlamı nedir? Takip edildiğimizin farkındayız.

Evet, bakın, mesela, Google Hacking diye bir kitap var, 2 bölüm. Bunu ben üniversitede derslerimde okutuyorum öğrencilerime. Biz İnternet'te aramayı bilmiyoruz. Bakın, ülkenin en yüksek teknoloji şirketlerini yöneten şirketlerimizin CEO'ları bile bilmiyor, bunu bir ortamda sordum kendilerine. Ha, bilmek zorunda mı? Değil ama gerçekten bilmiyoruz. Google bize dehşet bir ortam sunuyor aramak için. Bakın, Millî Eğitim Bakanlığıyla ilgili küçük bir örnek olsun diye: Site:meb.gov.tr yazıyorsunuz; burada dosya tipi, uzantısı doc olan, gizli olan belgeleri bana listele diyorsunuz. İşte

listeler, görebilirsiniz. Google yapıyor bunu, ben yapmıyorum bakın, açık. Arkadaşlarımız farkında olmadan gizli belgelerini oraya koymuşlar, Google endekslemede alıyor, buradan görünebiliyor. Bakın Türkiye'nin…

ALİ ERCOŞKUN (Bolu) – Gizli olduğu hâlde tıklayınca açılıyor mu?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Tabii, tabii, indirebiliyorsunuz. Yani öyle şakası yok bunların.

Bakın, burada gizli dosyaların neler olduğunu görebilirsiniz. Sadece ben size 2-3 tanesini göstereceğim.

ŞUAY ALPAY (Elâzığ) – Hocam, hacker'lama yapmadan olan şeyden mi bahsediyorsunuz?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Hack'leme yok, ben sadece…

ŞUAY ALPAY (Elâzığ) – Sadece arama yaparken.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Bakın, arama yerine "site: meb.gov.tr filetype:doc gizli" yazıyorum o kadar, otomatik listeyi veriyor. Bakın, Türkiye'de dışarıya ihracat yapan bir şirketimizi tesadüfen, bir görevlendirmeyle, TÜBİTAK görevlendirmesiyle denetçi hakem olarak gittim. Gitmeden önce bir bakayım dedim. İnanın veri tabanları, şifrelerini Google'den gördüm, kendilerine ifade ettim. Ya dedim ki: "Siz veri tabanı satıyorsunuz, şifreniz…" "Hocam inanmıyorum!" dedi ya. "Gelin bakalım." dedi. Bilgisayar mühendisi arkadaşım "Hocam, ben bu mesleği bırakıyorum." dedi. Bu iş böyle bir iş. Farkında değiliz bakın, bu dünyanın gerçekten farkında değiliz, karşıda nasıl bir teknolojiyle uğraşıyoruz. "Google mühendisliği diye bölümler açılmalı ülkede." diyoruz yani biz bazı yerleri kapatıp artık bunlara odaklanmalıyız. Bu aynen, Başbakanımızın "Kendi arabamızı üretelim." hedefi gibi kendi arama motorlarımızı, kendi Facebook'larımızı, kendi altyapılarımızı oluşturmak zorundayız, bu hedeflere ihtiyacımız var ülke olarak. Yoksa kendimizi analiz edecek verilerimiz yok. Bize dışarı ne söylüyorsa onları biliyoruz ama kendimizi de analiz etmeliyiz ülke olarak gelişmek istiyor isek. Bunlara da yatırım yapmalıyız. Ya, şu anda FATİH projesi önemli bir proje ama içinin doldurulması gerekiyor bu tür teknolojilerle; var, çalışmalar var, bunları biliyorum ama daha çok çalışılması gerekiyor. Genç nüfusumuzu bu alana kaydırıp bu bacasız teknolojiden faydalanmak zorundayız. Evet, mesela, yine, devlet uzantılarına, gov.tr uzantılarına baktığımızda bir indeksleme ile admin dizinlerine erişebiliyorsunuz. Bu çok basit, bakın, sadece aramaya öyle yapıyorum bunu. Evet, burada bir örnek: Bakın, bu kez dosya tipi xls yani uzantısını da söylüyorsunuz. Kayseri Kadın Doğumla ilgili Baştabipliğin bir şeyini İnternet'ten görebilirsiniz. Bakın, Google söylüyor, ben söylemiyorum. Şimdi size soruyorum burada Komisyon olarak: Bu hack'leme midir, değil midir? Özel hayatı ben ihlal mi ediyorum şimdi? Bunları araştırıyorum. Şimdi, kişilerin veya kurumların hiç mi burada suçu yok? O belgelerini, bilgilerini oraya

koymayacaklar. Ben burada tesadüfen gördüm ama çok farklı bilgiler, belgeler de var, onları burada söylemiyorum ama burada tesadüf birkaç tane bilgiden bahsediyoruz. Ben size sadece 3 tanesini söyledim ama bunun yanında müthiş hizmetleri var. Mesela, Google'ın Cash hizmeti var. Şimdi, bir davalık konu olduğu için burada bunun bilinmesinde fayda olduğunu gördüğüm için bunu ifade ediyorum. Bir yere bir alımla ilgili ilan veriliyor. İlanda jüri seçiyor, şunlar ilan ediliyor ama sonra İnternet'te web sayfasından o liste düşürülüyor, değiştiriliyor, yayınlanıyor tekrar ama birisi görüyor bunu. Google'ın Cash hizmeti var, Google'ın Cash'ine düşüyor, Google Cash'ten o listeyi görebiliyorsunuz ve mahkemede kaybetti davayı. Neden? Google'ın bu hizmetini bilmediğimiz için. Yani, teknolojinin hakikaten bilinmeyenleri çok ama artıları da çok, şeffaflaşma için de güzel bir şey. O kişiler de o yamukluğu yapmayacaklar.

ERDAL AKSÜNGER (İzmir) – Hocam bu formu da incelediniz değil mi?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Evet, çok detaylı bakmasam da evet, yani.

ERDAL AKSÜNGER (İzmir) – Hani şimdi İnternet üzerinden yapıyor. Ama hangi siteye girdiğinizin bir önemi yok zaten. Hangi siteye girerseniz girin, Google'a girsen de girmesen de.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Evet, bu sadece küçük bir örnek yani. Binlerce arama motoru var, bakın, 1 milyonun üzerinde arama motoru var. Ben sadece burada ücretsiz olanlardan birisini gösteriyorum ama ücretlileri de var bunların. Parayı verin, bakın ne derin aramalar yapıyorlar. Bir de o var, biz daha o kısma hiç bakmadık. İçimizde var mı hiç paralı arama yapan arama motorlarında?

YILMAZ TUNÇ (Bartın) - Parasız varken paralı niye yapalım.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - Ama bir de paralı yaptırın o zaman.

YILMAZ TUNÇ (Bartın) - Parasızlar zaten derya gibi.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Derya, evet ama bir de diğer tarafa bakalım, bu gölse o denize de bakmak gerekiyor.

Evet, amacım, burada, sadece yani ihlallerin çerçevesini biraz böyle elektronik ortamlarda bilgilendirerek Komisyonu daha farklı belki… Mesela, sosyal ağlar, bundan çok bahsetmeme gerek olmadığını düşünüyorum. Mesela, burada düşünüyoruz, sosyal ağlara da, her şeye kafa taktınız mı araştırma yaptık yani her taraf ihlal dolu yani bir daha sosyal ağı kullanmazsınız bunları görünce ama ben kullanıyorum bu arada onu söyleyeyim. Teknolojiden kaçışımız yok, kullanacağız ama tedbirimizi de alacağız.

Mesela, yine, özellikler var, yaş sınırı. En çok ülkemizde gördüğümüz yaşını büyütüp İnternet'e giren çocuklarımız var çünkü belli yaşın altını kabul etmiyor kayıtlarda sistemler. Onun için,

çocuklar yaşını büyütüp ne yapıyor? Sistemlere erişebiliyor. Burada gördüğünüz, Facebook'ta yüzde 13 oranında olduğu görünüyor.

ŞUAY ALPAY (Elâzığ) - Hocam, bununla ilgili bir şey sorabilir miyim?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - Buyurun.

ŞUAY ALPAY (Elâzığ) - Bilgi çağında mesela sosyal ağlarda şeyi geçtiği zaman bir şeyi sormak istiyorum, tam denk geldi. "İstenmeyen e-postalar ve bot saldırıları." dediniz Şimdi, bütün bunlar tamam. Hiç yazmadığım hâlde, diyelim ki kendi bilgisayarımda bana ait olmadığı hâlde benimmiş gibi bir bilgi ve belge de üretme de mümkün herhâlde anlaşıldığı kadarıyla.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Yani, şöyle bot saldırılarında bilgisayarınızı saldırganlar ele geçiriyor, istediği zaman erişip oradan saldırı yapabiliyorlar.

ŞUAY ALPAY (Elâzığ) – Yani, ben öyle bir şey yazmadığım hâlde, yazmışım gibi bir mail, bir metin, bir bilgi de üretiliyor anlaşıldığı kadarıyla.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - Tabii ki, saldırgan sizin adınıza üretip gönderebilir. Onu söylüyor iseniz evet. Yani, burada çok önemli bir hususu hatırlattınız ama unuttum kusura bakmayın çünkü çok… Evet, sosyal ağlarda durum bu.

Şimdi, baktığımızda standartlarımız var. Bilgi güvenliği standartları artık 27 bin serili, bunlar daha spesifik. İşte, kritik altyapıların güvenliği şu anda mercek altında, ülkede de çalışılıyor, Siber Güvenlik Kurulu kuruldu, alt tarafta kurullar oluşturuluyor, çalışmalar başladı. Buna da hem Gazi Üniversitesi olarak hem Bilgi Güvenliği Derneği olarak büyük katkı sağladığımızı ifade edeyim. Ulusal ve uluslararası konferanslar, çalıştaylar yaparak ülkemizde bu farkındalığı oluşturmaya çalıştık bu arada. Kısaca reklam gibi oldu ama bunu da söylemekte fayda var diye düşünüyorum.

Şimdi, yeni çözümler kullanılıyor tek taraflı, bilgi bir tek yönlü. Diyotlar tek yönde iletim yaparlar, ters yönde de sızıntı akımları vardır ama burada da tek yönde bilgi aktarırlar ama ters yönde bilgiyi göndermeyen yaklaşımlar şu anda kullanılıyor. Kısıtlı kullanım sunan işletim sistemleri var. "Benim bilgisayarım her işi yapsın, her yazılımı olsun." diyorsanız tehdit altındasınız. Ne işi yapacaksanız onun için ihtiyaç duyduğunuz yazılımları, ihtiyaç duyduğunuz işletim sistemlerini kullanacaksınız.

"Şifre" diyoruz. Biz hâlâ şifredeyiz ama dünya ise cümlelere geçti. "Password" değil, "pass-sentence", cümleler şeklinde artık şifreler var. Şimdi, biraz önce "spam" dedi. Gazi Üniversitesinde bilgi işleme bakıyorum üç buçuk aydır. Hocalarımdan çektiğim kadar hiçbir şeyden çekmedim. Bunu, lütfen, kayıtlara almayın da şey olmasın.

BAŞKAN - Girdi Hocam kayıtlara.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Lütfen, basından -off the record- bu da benim kişisel ricam olsun Sayın Başkanım müsaade ederseniz.

BAŞKAN - Basın mensubu arkadaşlar buna hassasiyet gösterirler.

YILMAZ TUNÇ (Bartın) - Basın kişisel ricaya bakmaz Hocam.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - Bakmaz mı diyorsunuz?

YILMAZ TUNÇ (Bartın) - Hiç affetmezler.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Pekâlâ doğruyu her zaman aktaralım. Hocalarımız şifresini kaptırıyorlar. Dışarıdan erişildiği için şifreyle dünyaya mesaj gönderiyor, Gazi Üniversitesi spam listesine alınıyor, mesaj gönderemiyoruz. İnanın geceleri oturup spam listelerinden Gazi Üniversitesi ismini temizlemekten yoruldum. Şimdi, politika geliştirdik, bundan sonra katı kural uygulamayanı sistemden atacağız. Şimdi, politika geliştirdik, yazılı hâle getirdik bunları çünkü biz bunu ilk gün de yapabilirdik bütün herkesi ama yazılı bir kuralımız olsun, politikamız ona göre bunları uygulayalım. Geniş, 16 sayfa kuralımız var şu anda. Bunları uygulayarak hocalarımızın güvenli hizmeti alması ve sunmasını sağlayacağız.

Evet, mesela, bilgi çağında, havaalanlarında -Amerika'nın bir uygulaması, bilmiyorum bunu bildiğinizi düşünüyorum 19 Ocak 2013'te 200'e yakın havaalanında 40 milyon dolar harcanarak yapılan- X-ray'lerden geçince kişinin düştüğü hâle bakın. Şimdi, bu resimlere müthiş para verecek kişiler olabilir. Şimdi, X-ray'den geçerken görülen… Şimdi, Haziran 2013'te bunu kaldıracaklarını ifade ediyorlar ama bu cihazların farklı amaçlar için de kullanılabileceğini… Sadece gezerken ilginç geldiği için sizlerle paylaştım, İnternet'ten buldum ben bunu, hakikaten benim de çok ilgimi çekti ama bunun daha ötesi iki yıl önce geliştirdikleri niyet okuyucuları var Amerika'nın. Yüzde 100 kişinin niyetini algılıyor, yüzde 100. Ne olabilir? Amerika'yla ilgili bir hassasiyetiniz var mı, yok mu? Düşmanca bir tavır içerisinde misiniz? Gümrükten girerken 38 farklı sensörle algılıyorlar, kişinin niyetine göre de sorguluyorlar arka tarafta ve bunu iki buçuk yıl önce yaptılar ve İnternet'ten bulabilirsiniz. Bakın, niyetimizi okuyorlar, bırakın şeyi. Yani, tabii ki ülke terörü korku olarak gördüğü için buna yatırım yapıyor. Sadece biyometriye 1 milyar dolar yatırdılar biyometrik alanda çalışma için.

ŞUAY ALPAY (Elâzığ) - Bu cihazlar çalışmaya devam ediyor mu Hocam?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - Haberlere göre evet 200'e yakın havaalanında. Başlangıçta 43 havaalanına kurduklarını, belli bölgeler seçtiklerini şu anda 200 havaalanını… Son, güncel veriler bunlar. Ben de İnternet'ten bulduklarımı sizlerle paylaşıyorum.

ERDAL AKSÜNGER (İzmir) – Hocam, biyometriye geçtiler, şöyle, herkes biyometrik olsun istediler. Bize de dayattılar o ülkeye de dayattılar. Herkes öyle olsun istediler. Özellikle öyle yaptılar.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Evet yani doğru hızlı geçiş oluyor ama Amerika daha fazlasını yapıyor, on parmak alıyor, yabancıların on parmağını da alıyor. Mesela, beni gümrükte konuşturuyorlar, eminim, arkada yalan makinesi mi var, ne var. Ben de "Ben Profesörüm, sorduğunuz soruyu çok net anlıyorum." diyorum. "Sen konuşma, sorduğumuz soruya cevap ver." diyor. Aynı soruyu üç kez soruyor bana, arkada başka şeyleri olduğuna eminim.

MİHRİMAH BELMA SATIR (İstanbul) - Bu size özel mi yoksa bütün Türklere özel mi?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Ben kendimde gördüğümü paylaşıyorum sizinle yoksa…

MİHRİMAH BELMA SATIR (İstanbul) - Sizi biraz şey gördüler herhâlde.

YILMAZ TUNÇ (Bartın) – Çıkış noktaları…

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Yani, ben sadece… Sorguluyorlar, haklı olabilirler ki herkes ülkesini savunuyor.

Evet, şimdi, burası aslında şöyle bir gözden geçirmeydi. Bundan sonra bu ihlali önlemeye yönelik olarak casus yazılımları kısaca sizlere anlatayım. Birkaç örnek verelim, geçelim. Casus yazılım aslında küçük kod parçacıkları. Bu yazılımlar kişilerin işte, haberi ve izni olmaksızın bilgilerini karşı taraflara, üçüncü taraflara veya yazılımı yükleyen taraflara aktaran küçük kod parçacıkları. Pek çok amaç için kullanılabilirler. Amaçlarından birisi şu olabilir: İşte, kişiyle ilgili bilgi toplamak, casusluk amaçlı olabilir, eşini izleme amaçlı olabilir -literatürde böyle yazdığı için size söylüyorum- kendini izlemek amaçlı olabilir, çocuklarını izlemek amaçlı olabilir veya iş verimliliğini takip etmek amaçlı olabilir. Mesela, ben kendimle ilgili bir örnek vereyim. Kendi makinemde casus yazılım kurulu. Ben casus yazılım diyorum ama izleme yazılımı. Şimdi, öğrencilerim, asistanlarım bazen makineyi istiyorlar, "Hocam, kullanabilir miyiz?" "Seve, seve." diyorum. "Ne yapacaksın?" diye soruyorum. "Hocam, bir seminer var, onu vericeğiz." "Tamam." ama makine nereye girdiğini raporluyor bana, ne sunulduğunu, ne yapıldığını makine raporluyor. Ben onun doğru söylemediğini görüyorum tabii, kendi makinemde o. Bakın, kendimi korumak amaçlı. Ondan sonra makinemi ona vermiyorum. Yani, kişinin yalan söylediğini bile buradan tespit edebiliyorsunuz.

Şimdi, pek çok tipi var. Bunlarla ilgili 2005'te bir çalışma yaptık "Casus Yazılımlar ve Korunma Yöntemleri" diye. Bugün -özür dilerim- sizlere o kitaptan birer örnek getirmek isterdim, özellikle Sayın Başkanım size. Çok özür dilerim, böyle, sunumu bile son dakikaya yetiştirdim -arkadaşımız biliyor- sizlere mahcup olmamak için, iyi bir sunum hazırlamak için uğraştım yoğun gündemim içerisinde, ümit ederim faydalı olmuştur ama daha sonra size ileteyim, bakılmasında fayda

var. Şu açıdan: 2006 yılında çıktı kitap. 2006'da çıktığında dünyanın en iyi casus yazılımlarıyla ilgili kitabıydı, bunu size ifade edeyim. Yani, inanın, Amerika'dan gelip satın aldılar kitabı ama Türkiye'de kitaba ilgi duyan yok. "Casus Yazılımlar ve Korunma Yöntemleri" diye. En ince detayına kadar orada anlatıyoruz pek çok şeyi. Bakın, yedinci yıldayız. Bununla da ilgili bir şeyi ifade edeyim, bankalarla ilgili olarak kayıtlara geçsin. Herhâlde kayda geçiyor değil mi Başkanım?

BAŞKAN - Geçiyor, geçiyor.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Bankalar Birliğine, Türkiye'de, özellikle casus yazılımlar ve bu bankacılık sistemiyle ilgili olarak bir çalışma hazırladık. Bunu Bankacılık Düzenleme Kuruluna gönderdim, tüm bankalardaki zafiyetlerle ilgili olarak, sağ olsunlar bir teşekkür yazısı aldık. "CMUK'un şu şeyin şu maddelerine göre, eğer, bu raporu yayınlarsanız hakkınızda gereğini yaparız." diye bana teşekkür ettiler. Tamam mı? Ülkemiz o noktadan bugün gerçekten çok iyi bir noktaya geldi. Bunda biraz tuzumuz olduysa ne mutlu bana ama ondan sonra çok büyük önlem almaya başladılar. Şu anda dünyanın en ileri bankadaki güvenlik sistemlerinin bizde olduğunu düşünüyorum. Cep telefonuna mesaj gelmesi falan, bunlar önemli değişiklikler, önemli güvenlik adımları.

Pek çok sınıflandırması var. Bu, 2006'da yaptığımız bir sınıflandırma. Eminim bu sınıflandırma daha çok güncellenebilir günümüzde ama size burada örnek olsun diye... Şimdi, bunlarla neler yapılabilir kısmı önemli. Bilgisayarınızda yaptığınız her türlü işlem rapor edilebilir. Bakın, bu, şu demek: Yazıcıya gönderdiğiniz yazı, bilginin ne olduğundan tutun da... Mesela, bununla ilgili bir sekretaryamız sürekli kâğıt tüketiyordu. "Ne yapıyorsun?" diyorum. "Hocam, çok iş veriyorlar." diyor. Sonra öğrendik ki tez çıktısı alıyormuş öğrencilere. Söylüyor bu yazılımlar, ben söylemiyorum, tez çıktısı aldığını söylüyor yazılım. Yani, bu, iş verimliliğini artırma için kullanılabiliyor. Burada, girdiğiniz sitelerden tutun, ekran görüntülerinizden tutun, her şeyi raporlayabilen yazılım bunlar "keylogger" diye başlangıçta biliniyor ama günümüzde de bilgisayarda "activity monitoring system" olarak ifade edilen bir yazılım. Çok küçük bir yazılım, her şeyi yapabilir bu yazılım, dehşet yazılımlar var, ücretsiz de indirip kurabilirsiniz ama kurmamanızı öneriyoruz. Bilmediğiniz şeyleri lütfen kurup kullanmayın.

Evet, tabii ki burada çocuklarımızla ilgili... Mesela benim de 2 tane kızım var, onların makinelerinde bunlar var, onlara bakıyorum. Kullandıkları kelimeye göre raporluyor yazılımlar. Ya, onlara karışmak değil ama kontrol altında tutmak zorundayız. Ya, şu anda güvenli İnternet hizmetiyle kısmen bunlar devre dışı kalabilir.

Şimdi, bakın, sadece size örnek olsun diye klavye izleme ve dinleme sistemlerini burada kısaca bir ifade edelim. Bakın, burada şekilsel de var. Bu şu kadarcık bir parça, İnternet'ten sipariş verip alabilirsiniz. Bilgisayarınızın arkasına takılıyor ve klavyeye bastığınız her türlü basım bilgisini içerisinde kaydediyor ve bir gün sonra da çıkartın, hiç fark edilmiyor. Bir gün dursa makine üzerinde bu

cihaz, ne vardır onun içerisinde sizce? O günkü yaptığınız, klavyeye bastığınız her türlü tuş basım bilgisi vardır. Peki, geldiğinizde, ilk tuşa bastığınız kelimeler neler?

ALİ ERCOŞKUN (Bolu) - Şifre.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - Şifremiz, tamam. Benim onu almam yeterli. Hoş, onu almama bile gerek yok, zayıf şifre kullandığımız için mesela, bir şifrenin kırılmasının bir saniye sürdüğünü söylesem inanmazsınız. Burada bir bakın, saniyede kırılabilen şifreler kullanıyoruz.

Pekâlâ, bu başka. İnanın, ben de bunu hep empedans uygunlaştırıcısı zannederdim gördüğümde.

HASİP KAPLAN (Şırnak) - Hocam, Voynich alfabesini kullansak hiç kimse çözememiş o alfabeyi. Öyle derler çözülemeyen bir dil, bir alfabe.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - Evet, var, doğrudur, doğrudur ama kim anlayacak onu o zaman?

HASİP KAPLAN (Şırnak) - Bilişimciler anlar.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - Yok, mutlaka birilerinin de anlaması lazım karşılıklı.

ERDAL AKSÜNGER (İzmir) - Yazılım değil, önce, öyle bir yazıyı yazmak lazım.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Şimdi, bakın, burada gri gördüğümüz kısım da bir klavye dinleme aparatı. İnternet'ten 5 dolara alabiliyorsunuz bu arada. Bunları basınımız herhâlde yazmaz, duyarlı bir basına sahip olduğumuzu düşünüyorum.

HASAN ALİ ÇELİK (Sakarya) - Kesinlikle, ser verip sır vermez!

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Şimdi, bunlar çok küçük cihazlar, çok kolaylıkla elde edilebilecek cihazlar. İşte, farklı teknikler var ama 2005 yılında 500'den fazla casus yazılım vardı, şu anda sayısı artık milyonlara yaklaşmış olabilir diye düşünüyorum. Basılan tuşları izleyip kaydedip bunları e-posta veya ftibi'lere gönderebiliyorlar. Mesela, televizyonda duyarlılık artsın diye, canlı yayında, bilgisayarınıza ilk girdiğinizde tuş basım bilgilerinin cep telefonuna sms olarak atılmasıyla ilgili bir canlı demo yapmıştım yani farkındalık artsın diye üç yıl önce. Yani, tehlikenin boyutunu ortaya koymak için ama herhâlde faydalı oluyordur diye düşünüyorum bilinci artırma adına.

Evet, bakın, bu casus klavye. Tuş basım bilgilerinizi başka noktalara aktaran, içerisinde bluetooth vericilerle haberleşen bir sistem, 800 lira. İnanın Microsoft klavyeyle hiç ayırt etmeniz mümkün değil. Bakın, bu, bir diğeri. Bu da casus klavye. Bastığınız anda tuş basım bilgilerini başka yerlere gönderen, 890 liraya satılan casus bilgisayarlar var. Şimdi, bunların örneği o kadar çok ki,

bunları artırabiliriz. Bu sadece size bu alanda bilgi sahibi olmanız için, mutlaka bilginiz vardır, ben üzerinden şöyle hızlıca bir geçiyorum.

Şimdi, yazılım olarak baktığımızda bunlar daha tehlikeli. Sistemi her etkili izleyen yazılımlar ve raporlayan yazılımlar. Biraz önce dedik, yaptığınız her işlem raporlanabilir başka taraflara. Şimdi, bu yazılımları da, bunu yapan yazılımları şöyle bir derecelendirmiştik, puan verdik hangisi en iyi bu işleri yapıyor diye ama siz de girip İnternet'ten bakabilirsiniz.

Bunların nasıl yapıldığı ile ilgili bazı detaylar var, teknik olarak özellikle bilmek istediğinizi söylemişsiniz. Mesela dinleme türleri, kopyalama yöntemi var, klavye tablosu yöntemi var, klavye dinleme bağımsız yaklaşımı var. Bunları önlemeye yönelik de tedbirler mutlaka var ama esas, burada çözüm anti-keyloggerler yani bilgisayarlarınıza yüklediğiniz işte, anti-casus, anti-spam, anti-virüs yazılımlar gibi bu da anti-keyloggerler var. Bilgisayarınızda bir şey oldu mu bunları önleyen yazılım bunlar.

Çözümler de var: Kimliklendirme yöntemi, kopyalama yöntemini durdurma gibi, klavyeden gelen verileri takip etme gibi, sanal klavye gibi. "One-time password" demek yani "bir kerelik şifre" -bazı bankalarımız kullanıyor- anlık kartlar var, sms mesajları -kullandığımız- ve mobil elektronik imza bunlardan bazıları.

Şimdi, telefonlar var. Mesela, telefon dinlemede casus kulaklıktan tutun da farklı türleri var. Telefon dinlemeye, bunlarla ilgili canlı demo yapıldığını söylediği için bunları biz iyi yapmıyoruz ama fiyatları İnternet'ten kolaylıkla bulabilirsiniz. Şimdi, çiçeklik dinlemeden tutun da -artık işi abarttıklarını- çantadan, duvar saatine yani pek çok yere dinleme cihazları konabilir yani yazılımsal olarak da.

İşte, akıllı telefonlar. İçimizde akıllı telefon kullanmayan bir vekilimizi gördüm. Var mı başka kullanmayan merak ettim.

HASİP KAPLAN (Şırnak) - Var kullanmayan vekilimiz.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Hayır, hiç kullanmayan vekilimiz.

HASİP KAPLAN (Şırnak) - Ahmet Türk kalp pili olduğu için hiç kullanmıyor Hocam.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Ha, o özel bir durummuş ben de şaşırdım.

HASİP KAPLAN (Şırnak) - Onun dışında hiç yok.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Pekâlâ, akıllı telefonları da hızlıca bir gözden geçirelim. Neden akıllı telefon kullandığımızı söylememize buraya gerek olmadığını düşünüyorum ama saldırganların hedefleri bir defa kişisel verileri elde etmeye çalışan saldırılar yapmak veya bu bilgileri sadece saldırgan olarak değil, farklı amaçlar, ticari amaçlar için kullanmak, reklam yapmak, kişilere farklı alternatifler sunmak, işte -

biraz önce operatör örneği verdik- farklı, uygun teklifler sunmak, "Şu tarifeye geçerseniz daha sizin için uygun olur." gibi şeyler de olabilir, bunu nasıl algılıyorsanız. Mesela -burada kayıtlara geçmesini rica edeceğim- ben bir İnternet geniş bant abonesiyim bir şirketin. İnanın, sözleşmemin bitmesine bir hafta kala beni diğer bütün operatörler aradı, eminim sizi de aramıştır. Ya, demek ki bu operatörümüz veri tabanına sahip olamıyor veya alınıyor, satılıyor başkalarına. Ya, o kadar çok rahatsız edildim ki hakikaten nefret ettim geniş bant aboneliğinden bunlar yüzünden. "Ya, aramayın kardeşim. Kayıtlarınızda yok mu? Beni aramayın." diyorum. Yine arıyor "Biz şuyuz, buyuz, bilmem neyiz." Şimdi, kesildi, üç ay geçti üzerinden. Yine, "Başka şey olabilir, ucuz yaparız, ücretsiz yaparız…" Böyle, çıldırtıyorlar. Sigarayı bırakmamla ilgili olarak çok telefon alıyorum. Hakikaten rahatsız ediyor. Ya, ben sigara kullanmıyorum ama özellikle arıyorlar beni "Sigarayı bırakın." diye. Nasıl o bilgiyi edindiler?

HASİP KAPLAN (Şırnak) – Arama motorlarından otomatik geliyor.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - İşte bilmiyorum. Bunun gibi şeyler. Eminin sizlerin başına daha çok geliyordur, sizler daha gündemde olan kişilersiniz, rahatsızlık da duyuyorsunuzdur, işimiz, gücümüz yok, akşama kadar telefon… Ya, bunların kayıt altına girmesini istiyorum ki bunların, eminim, çözülebilecek, önlemler alınabilecek yer burası olduğu için.

Evet, şimdi, saldırıları sınıflandırdığımızda bakın, cep donanım bazlı saldırılar var, jailbreak saldırısı var, yazılım merkezli saldırılar var, kullanıcı merkezli ve cihazdan bağımsız saldırılar var. Şimdi, bunlara baktığımızda mesela, bir cihazı bir yerde kaybedebilirsiniz veya çalınabilir veya veriler yok olabilir ama cihazlar akıllı, üzerinde hemen uygulaması var. "Find my iPhone" diyorsunuz hemen lokasyonu size söylüyor nerede olduğunu, "remote wipe" var, bunlarla lokasyon bilgisini söylüyor. Bir, Google'a giriyorsunuz "Yerinizi işaretleyelim mi?" diye soruyorlar size, hemen işaretliyorsunuz. Facebook'ta lokasyon bilgileriniz otomatik geliyor. Bakın, Twitter kullanmayan var mı içinizde?

BAŞKAN – Var, var.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Kullanıyorsunuz, kullanmayın.

Bakın, Twitter'dan kişinin lokasyonları tespit edilebiliyor, bunu benim lisans öğrencilerim çalışıyor proje olarak ve kişinin davranış modeli çıkartılabiliyor, nerelerde geziyor, mesajları nerelerden atıyor gibi. Bunları anlatıyorum ama tabii ki bunlar kişi istediği için oluyor, istemezseniz o şeyleri kapatabilirsiniz ama Facebook'ta "Ben şu anda buradayım, şu kafedeyim, buradayım veya şu tatil köyündeyim." deniyor bakıyorsunuz evi soyulabiliyor kişinin. Bu tür örnekleri gazetelerde çok okumuşsunuzdur veya Türkiye'de cinayet de işlendi bu tür konularda. Bunu da eminim size bilgileri aktarmışlardır.

İşte, jailbreak saldırısı, hakikaten bu en tehlikeli saldırı. Eğer jailbreak'li bir makine kullanıyorsanız çok tehlikeli olduğunu söyleyeyim size. iPhone bozulmuştu bir tamire götürdüm. Dedi

ki: "Hocam, jailbreak yapalım size ben 300 tane de uygulama yükleyeyim üzerine." "E, olur." dedim. "Bunu herkes istiyor mu?" diye biraz vatandaş olarak sohbet ettim. "Evet, Hocam, çok hoşlarına gidiyor uygulamaları görünce." Ama konuştuktan sonra gördüğüm, jailbreak olmayan makineye jailbreak yaptırıp bütün yazılımları yükleyebiliyorlar, uygulamaları. Gerçekten süper uygulamalar var, hayat kurtarıcı uygulamalar var içerisinde ama ihlal eden de var. Ha, bunun riski nedir? Yani, kişiye bağlı, o riski alıyorsanız kullanırsınız, almıyorsanız kullanmazsanız.

Evet, bu, sadece mesela yazılım merkezli saldırılar var, bazı vakalar var burada. Onları şeylerinizden görebilirsiniz ama burada iPhone üzerinde, iPhone Store'da yüklü olan yazılımlar üzerinde yapılan testlerde çıkan ihlalleri burada kısaca sizlere özetledim çünkü çok vekilimizin iPhone kullandığını bildiğim için özellikle de bunları buraya koydum, eminim paylaşırsınız diye düşünüyorum. Bilinen ilk iPhone virüsümüz de var. Kaç kişi anti-virüs yazılımı kullanıyor, anti-casus iPhone'larında? Merak ettiğim için. 1. Evet, kullanmamızda fayda olduğunu düşünüyorum.

Bluetooth saldırıları var, browser saldırısı var yani, bunlar, işte, maddi çıkar sağlamak için yapılan saldırılar, botnet saldırıları. Bakın, botnet önemli bir saldırı türü. İşte, biraz önce dediğimiz, hani, habersiz kesim dediğimiz kısım bu. Sizin cep telefonlarınız bir saldırı aracı olabilir ama farkında olmayız. Onun için, bunlara önlem almak zorundayız veya güvenilir yerlerden mutlaka uygulama indirmek durumundayız. Mesela, geçen gün yine bu Android'in uygulaması, CIA diye bir uygulaması var. CIA uygulamasında ben sizlerin telefonunu oradan elde edebiliyorum. Atıyorum, eğer, bir vekilimi tanıyor isem vekilim benim veri tabanına kayıtlı, o uygulama, eğer girmişseniz bütün veri tabanlarını ortak tutuyor. Daha girmeden arayan kişinin isminin kim olduğunu ben ismini bilmiyor isem orada söylüyor, sizi şu arıyor diyor mesela çünkü veri tabanlarını topluyorlar bütün telefonları, o veri havuzundan çekiyorsunuz. Ha, ihlal midir bu? Bence olmayabilir de ama ihlal de olabilir, nereden bakıyorsanız çünkü cep telefonumuzu herkese vermiyoruz. Sizler için büyük bir ihlal olabilir çünkü cep telefonu susmayabilir. Çok değerli bir arkadaşınız o uygulamayı yüklemiştir, "Yes." demiştir, o veri tabanını paylaştığı için sizin de cep telefon numaranız başkasına otomatik gitmiş olabilir. Dolayısıyla, bakın, iyi niyet, bende değil sadece ihlal, çevremdekilerin de dikkatli olması gerekiyor. İşte, en zayıf halka kadar güvendeyiz diyoruz. Hepimizin halkasının güçlü olması gerekiyor, hepimizin konunun farkında olması gerekiyor.

Burada bazı saldırılar var iPhone'a yapılan, bunlara da bakabilirsiniz diye düşünüyorum. Şimdi, burada… Bilmiyorum, süreyi çok aşmadık değil mi?

BAŞKAN - Yok, zamanımız var.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Şimdi, kişisel gizlilik ve mahremiyet nasıl sağlanır? Ben de düşüncelerimi sizlerle burada paylaşmak istiyorum. İşte, kişisel mahremiyet veya kişisel gizlilik dediğimizde aslında bir döngü var, buna kişisel gizlilik ve mahremiyet yaşam döngüsü olarak bakabiliriz. İşte, bedensel ve yaşam alanı

mahremiyeti konusu burada yok ama iletişim ve bilgi veya veri mahremiyeti aslında buradaki temel konulardan birisi diye düşünüyorum. Şimdi, buraya odaklanmıyoruz ama bunun bir bütün olduğunu ifade etmekte fayda var. Sadece, biz buraya odaklansak da bu büyük resmi görmemiz gerekiyor.

Şimdi, özel hayatın gizliliği, "ÖHG", öyle kısalttım. Şimdi, taraflara şöyle bir bakıyorum: İnsan var içinde, teknoloji var, teknikler var, hukuk var destekleyen, politika ve standartlar var, iş birliği, koordinasyon ve eğitim var. Şimdi, isterseniz tek tek bakalım.

İnsanı biraz değerlendirdiğimizde eminim sizlere de çok şikâyetler gelmiştir, ülkede bir paranoya var. Dün bir haber programında vatandaşa soruyorlar, herkes dinlendiğini düşünüyor. Var mı burada dinlenmediğini düşünen mesela? İşte, bu kötü. Dinleyenler kimler yani devlet mi dinliyor başkaları mı?

HASİP KAPLAN (Şırnak) – Bu paranoya değil ama bir gerçek Hocam.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Gerçek mi? Ha ben onun için şaşırdım.

HASİP KAPLAN (Şırnak) – Paranoya değil yani bu kadar anlatımınızdan sonra.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Ya ben kaldırayım yani ben, şöyle, dinlenebilir miyiz? Evet ama dinlemeyi kimlerin yaptığını iyi analiz etmek gerekiyor.

Şimdi, biz dinleme dediğimizde sanki devlet dinliyor, hep o gündeme geliyor ama devletin dışında bunu istihbarat servisleri dinleyebilir, yabancılar yapabilir. Bunlar için altyapı var, teknolojiler var. Esas tehlike bu, devletin dinlemesi değil diye düşünüyorum. O hukuk kuralları çerçevesinde dinleme yapıldığını kamuoyundan ben de öğreniyorum ama bu paranoyayı giderecek altyapıları kurmak herhâlde bu Komisyonun da görevlerinden birisi. Bundan çabuk kurtulmamız gerekiyor, paranoyadan kurtulup bu teknolojileri kullanarak bundan ülkeye nasıl katma değer sağlayabiliriz, ülkeyi nasıl geliştirebiliriz diye biraz daha çok kafa yormak gerekiyor. Kullanıcı olmadan, tüketiciden artık üretim veya üretici tarafına geçmemiz gerektiğini düşünüyorum. Şimdi, burada…

ERDAL AKSÜNGER (İzmir) - Ne üreteceğiz Hocam, onu da söylerseniz.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Pardon.

ERDAL AKSÜNGER (İzmir) - Ne üreteceğimizi de söylerseniz.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Bilgi. Ne üreteceğiz? Ha, dinlemeye, izlemeye yönelik olarak…

ERDAL AKSÜNGER (İzmir) - Önümüzdeki süreçle ilgili neler yapılması gerekir?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Ben anlatayım sonra sorularınıza… Olur mu Sayın Vekilim?

Şimdi, bilgi ve bilinç, tehditler ve önlemler burada önemli, farkındalık önemli, bilgi üretmek önemli, işte, etik ve ahlak burada çok önemli, güven ve denetim kısmı çok önemli, caydırıcılık burada hukuk çerçevesinde önemli, eğitim, tabii, burada teknoloji okuryazarlığı da çok önemli hâle geliyor. Hepimizin teknoloji okur yazarı olması gerekiyor yani bilinçli kullanım adına. Yani, biraz önce demiştik bir arama yaparken bir kelimeyi bile fazla girmemeliyiz hem kendimizi ifşa etmemek için hem de sistemler de arkada enerji harcıyor o kelimeleri aramak için. Mesela bir kelime aranırken bir kahve fincanını ısıtacak kadar enerji harcandığını sistemler rapor ediyor, literatürde bu var. Sosyal açıdan da bunlara dikkat etmemiz gerektiğini düşünüyorum.

Şimdi, teknoloji ve teknikler açısından baktığımızda, mutlaka çözüm sunan teknolojileri kullanmak zorundayız. Bunlar, işte anticasuslar, antivirüsler, antispamlar, antikeyloggerler gibi şeyler olabilir, firewall'lar gibi. Mümkün olduğu kadar teknoloji tarafımızı sıkılaştırmalıyız ve bu konuda AR-GE yapmalıyız yani kişisel verilerin korunması konusunda ülkede AR-GE yapmalıyız. Yani, neler olabilir? Bu kadar açık var, bakın, size bu kadar büyük bir çerçeve çizdim, veriyi analiz edeceğiz ama analizde bunların kullanılmaması için de teknoloji geliştirebilecek zekâmız olduğunu düşünüyorum. Bunlara biraz daha çok kafa yormalıyız diye düşünüyorum ve bu alanın teşvik edilmesi gerekiyor yani bilgi güvenliği alanının teşvik edilmesi gerekiyor. Ama, teşvikten kasıt, hem üreteceğiz hem de koruyacağız. Üretmeyen değerini bilmiyor ve koruyamıyor maalesef. İşte, fayda, zarar, maliyet analizini burada mutlaka yapmalıyız. İşte, bilgi seviyesi yükseldikçe, değer seviyesi yükseldikçe koruma seviyesinin de yükselmesi gerektiğini burada ifade etmek durumundayız. Teknoloji okuryazarlığı burada da önemli, bilinçli kullanım ve güvenli İnternet hizmeti var. Bakın, gündemde oldu, çok tartışıldı ama şu anda büyük bir hizmet olduğunu görüyorum, çünkü kullananlar, o habersiz kısım o kadar çok ki… En azından devlet korumasıyla veya çıkan kanunla, yönetmeliklerle bu destekleniyor, isteyen kullanabiliyor. Şu anda en azından tehdit ve tehlikeler o kişiler için, kullanan aileler için risk seviyesini düşürüyor, çünkü yazılımlar oradan geliyor maalesef. Girdiğimiz o uygunsuz sitelerden girilen veya haberimiz olmayan sitelerden sistemlerimize giriyor, girdikten sonra da artık bilgiler başka tarafa aktarılabiliyor.

Hukuk tarafı, tabii, kişisel verilerin korunması kanunu gündemde ülkemizde. Mecliste beklediğini düşünüyorum, bunun bir an önce çıkmasında fayda olduğunu değerlendiriyorum.

İş birliği, birimler ile kurumlar arası iş birliği kesinlikle şart, kişiler arası iş birliği bile şart. Bakın, biraz önce, iki arkadaştan birisi ihlal etti mi diğerinin verisi de ötekine kayabiliyor. Dolayısıyla, bilgiyi aktaracağız, iş birliği dediğimiz şey bu. Yani, güvenlik seviyem A seviyesindeyse diğerinin de A seviyesinde olması gerekiyor. Bu, ulusal ve uluslararası iş birliği gerektiren bir konu. Artık, İnternet'e girdiğinizde arkanızda şu anda 3,5 milyar İnternet kullanıcısı olduğunun farkında olarak sistemlere girmek gerekiyor. Tabii, burada, devlet, sektör, STK iş birliği şart. Bilgi güvenliği sektörünün ülkemizde de gelişmesi gerektiğini burada düşünüyorum çünkü sektör dinamikleri daha hızlı ilerlediği

için iş birliğinin daha çok arttığını değerlendiriyor. Üniversiteler tabii ki bu konuda da araştırma yapmak durumunda.

Şimdi, burada, "Neler yapılmalı?" dediğimizde, paranoyayı önlemek için mutlaka vatandaşın korkularına cevap verebilecek merkezler mi açarız veya sistemler mi kurarız, bunu bilgilendirme yerleri mi açarız, bunların yapılması gerektiğini düşünüyorum.

Tabii ki, biraz önce söylediğimiz güvenli internet hizmetine casus yazılımlarla ilgili kişisel verileri ihlal eden yazılımların belirlenip bu listeye alınmasıyla, bunlar kısmen önlenebilir diye düşünüyorum. Televizyonlarda yine eğitim, bilgilendirme, İnternet üzerinden, radyo, medya üzerinden bilgilendirmelerin yapılmasının artık faydalı olacağını düşünüyorum. Burada, yine, koruma bilincinde kişisel, kurumsal ve ulusal boyutta bu işlerin ele alınması gerektiğini burada değerlendiriyorum. Konuyla ilgili birimlerin, kurumların ve kuruluşların da ortak çalışması, özellikle STK, kamu, üniversite ve özel sektörün birlikte çalışması ve çözümler üretmesi gerektiğini burada düşünüyorum. Bilgi güvenliğinin yüksek seviyede olması için de mutlaka millî yazılımlar ve yöntemler geliştirilmeli. Sakın, burada şu anlaşılmasın: Kişileri izlemek, dinlemek için millî yazılım diye bir şey yok yani bu güvenliği sağlamak için. Zaten, güvenliğiniz sağlandı mı arka tarafta pek çok problemin giderileceğini düşünüyorum. Üniversite, sivil toplum bu konuya daha çok duyarlı olarak kişisel verilerin korunması ve mahremiyeti konusunda yine iş birliği yaparak bu konuda ortak çalışmalar yapması gerektiğini değerlendiriyoruz. Belki burada, bilgi toplumu ve güvenliği bakanlığı gibi, ulusal güvenlik bakanlığı gibi bir bakanlığın ülkemizin artık olmazsa olmazlarından olduğunu düşünüyorum. Bağımsız denetim organları belki kurularak bu paranoyaların giderilmesine belki katkı sağlanabilir.

Evet, burada sonuç olarak, bilgi güvenliği ve kişisel verilerin hakikaten çok ciddi bir konu olduğunun hepimiz farkındayız, bu Komisyon da onun için oluşturuldu, çözüm bulmak için. Neyi koruyacağımızı bilmemiz gerekiyor, neyin kişisel verimiz olduğunu, mahremiyetimiz olduğunun farkında olarak ona göre bir koruma seviyesi belirlememiz gerekiyor. Nasıl korunacağımızın veya korunmayacağımızın da farkında olarak bu işin yürütülmesi gerektiğini düşünüyorum. Uygulama safhası önemli, bilmek yetmiyor, bir şeyi bildiniz mi mutlaka uygulayıp onun tedbirini almak zorundasınız. Burada, gözetleme, izleme ve denetimi -sakın- kişisel, devlet izlesin gibi değil, genel olarak sistemlerin de izlenmesi yani izleyen bir sistem varsa onu da izleyecek farklı sistemler kurulabilir ama onda da dikkatli olunması gerekiyor. Çünkü, bu, ulusal mahremiyete de dikkat etmek gerekiyor sadece kişisel, kurumsal değil, ulusal mahremiyet de bu konuda önemli.

İnsan eğitim ve teknoloji birlikteliği sağlanarak bu işin püf noktasında, bu farkındalığımızı artırmamızın faydalı olacağını düşünüyorum.

Teşekkür ediyorum.

BAŞKAN – Biz de teşekkür ediyoruz Hocam.

Arkadaşlarımızın soruları olabilir.

Sayın Kaplan…

HASİP KAPLAN (Şırnak) – Teşekkür ediyorum Sayın Başkan.

Hocam, teşekkür ediyoruz yani bir korku filminin içinde sırlar, gizemler, rekabetler, takipler, izlemeler… Yani, her şey sızdırılan bir sunum oldu. Tabii ki sorular da buna göre… Ben birkaç teknik soru soracağım: Yargı, doğru bilirkişiyi neden bulamıyor? Soru-cevapları toptan alırsanız… Yargı, doğru bilirkişiye bir türlü ulaşamıyor. Bu konuda bir sıkıntı var.

Bu bilişimdeki sözleşmeler var; imza, kontratlar, bankalar, cep telefonlarındaki aramalar, şirketler, alışverişler, bunların güvenliği ve geçerliliği konusu var.

Google'daki sansür… Ülkeler sınırlarıyla bağlı, tam bir sansür sağlanabiliniyor mu? Yaygın bir arama motoru olması nedeniyle soruyorum. En çok sansür uygulayan ülke hangisi? Yani, bu, bilgi erişimi olduğu için, merak ettiğim için soruyorum.

Bir bilgisayarı izlemek mümkün IP numarasından.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Doğrudur.

HASİP KAPLAN (Şırnak) – Bir yurtta kalıyoruz ama 50 tane öğrenci bir bilgisayar almış, herkes kullanıyor. Onu nasıl tespit edecekler? Bu, benim kafamda bir soru işareti.

Bu casusluk davalarında hâlâ soğuk harbin öncesi gibi fotoğraf çekme delilleri falan kullanılıyor yani ilkel bir iddianameler tomarıyla karşılaşıyoruz. Bunca iletişim, bunca bilişimin içinde bu casusluk konularının bu kadar ayağa düşmesinde, bu konuda ciddi bir eğitimin olmayışının katkısı var mı?

Türkiye, kendi arama motorunu, bilgisayarını, cep telefonunu neden yapamıyor? 75-76 milyonda kafası çalışan… Ciddi AR-GE bütçeleri veriliyor. Ben bu işin başından beri, 2007'den beri takip ettiğim için söylüyorum: Başlangıçlarda teknoparklar vardı, şeyler vardı ve doğru dürüst bir bütçe ayrılmıyordu. Şimdi, yüzde 2'lerde bir bütçe ayrılıyor, Avrupa Birliği fonlarından ayrılıyor. Buna rağmen yazılımda ve diğer konularda, üniversitelerle ciddi bir iş birliği yapılamadığı için mi sonuca varılamıyor?

1 milyonun üzerindeki arama motorunun varlığından bahsedildi ama kullanılan birkaç tanesi. Bu da denetimsizliği, denetimi zorlaştırmıyor mu mutlak bir açığı veriyor?

Bu havaalanı X-ray'ları yeni galiba, kaydedici X-ray'lar bunlar. Bir de en son, kimliklerimiz çıktı, retina izleme konusu. Oysa, ben bunu on beş sene önce avukat olduğumda, uygulamada birkaç yerde görmüştüm. Göz retinası var, parmak izi var, klasik parmak izi var….

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Şu anda avuç içi var.

HASİP KAPLAN (Şırnak) – Şimdi, gelişmiş teknolojilerde, F tipi cezaevlerinde de açma-kapama için kullanılan bir sistem var, geçici şifrelik. Türkiye bunları geliştirme konusunda teknolojik

olarak niye bir zaaf yaşıyor onu anlayamadım, üniversitelerimiz mi yetersiz? Casus yazılımlar konusunda bizim de hanemize hackerler dışında bir şeyler düşüyor mu yani bizde de bir yazılım merakı var mı yani üniversitelerde meraklılar?

En güvenli telefonlar hangisi? Yani, hakikaten, akıllı telefonları birer dinamit gibi cebimizde dolaştığı noktasına vardık yani bunun en sonunda. Ama, mutlaka bunun bir önlemi de olması lazım, sonuçta bir bilgisayar bu da. Hangi antivirüs programları bu tür konularda daha faydalı olabilir, bizim böyle bir çalışmamız var mı?

Paranoya olayını, vatandaş yaratmadı, devletin tepesi yarattı. Anayasa Mahkemesi "dinleniyorum" dedi, Genelkurmay "dinleniyorum" dedi, Cumhurbaşkanı "dinleniyorum" dedi, Başbakan "dinleniyorum" dedi, üst yargı "dinleniyorum" dedi, milletvekilleri "dinleniyorum" dedi. Vatandaş da "Madem ki herkes dinleniyor bizde haydi haydi dinleniyoruz." yani bu kadar basit. Şimdi, burada fail kim? Fail, maalesef, birinci derecede her zaman devletin istihbarat ve emniyet güçleridir. En basit gerekçedir, güvenlik gerekçesiyle izlemek, vatanseverlik gerekçesiyle izlemek. Diğerleri; kaçakçılık, kâr amaçlı özel şirketler, kıskançlık nedeniyle eşini takip etmeler, dedektiflik, magazinel, bunlar istisna ama bugünkü sunuşunuzda bana bir üye olarak kafamda yeni bir paragraf açtığınız için teşekkür ediyorum Hocam. Biz, hep hukuk ve uygulama boyutuna ağırlık vermiştik. "Hukuk nasıl bir düzenleme olmalı?" noktasında gidiyoruz, o iyi gidiyor. Uygulamada da "Nasıl dinleniyoruz?" konusunu dinlenerek öğreniyoruz. Ama, eğitim noktasının çok zayıf kaldığını ifade ettiniz…

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Sayın vekilim, çok özür dilerim. Söylediklerinize kalemler yetmedi, yazamadım kusura bakmayın.

HASİP KAPLAN (Şırnak) – Hayır hayır, sonra da cevap verebilirsiniz.

BAŞKAN – Hocam, tutanaklara geçebiliyor, sonra gerekirse alabilirsiniz direkt.

HASİP KAPLAN (Şırnak) – Eğitim konusunda, bilişim dersi olarak… Bir bakanlık bile önerdiniz, bilişim ve güvenlik bakanlığı. Hakikaten, düşündüğümüz zaman milyarlar, bankalar, şirketler, devletin özel güvenliği, uçaklar, yazılımlar ve ciddi bir şekilde yürütmenin düşünmesi gereken bir alan. Ben, ondan öte, eğitim alanını… Çocuklarımız daha 5 yaşında bilgisayarı kullanıyor, 4-5 yaşında oyunlara başlıyorlar. Ana sınıfından başlayarak bu bilişimin, hukukun, dersi verilmesi gerekiyor mu gerekmiyor mu? Verilirse mecburi bir ders olarak çünkü herkesin hayatında… İnanın, hangi köye giderseniz, elektriğin gittiği her yerde ki daha çok ihtiyaç duyulan bir olay olarak çıkıyor… Eğitim açısından önerileriniz… Çünkü, eğitim, bilgilenme demek; bilgilenme demek güvenlik sağlama demektir, önleme demektir. O anlamda önemli.

Teşekkür ederim.

Başkanım, teşekkür ederim.

BAŞKAN – Teşekkür ediyorum.

Sayın Ercoşkun…

ALİ ERCOŞKUN (Bolu) – Evet, teşekkür ederim Sayın Başkan.

Öncelikle Hocamıza çok teşekkür etmek istiyorum. Gerçekten, bugüne kadar aldığımız sunumların bence herhâlde en iyisi, en kalitelisi, en detaylısı oldu. O anlamda gerçekten teşekkür ediyorum.

Birkaç konuyu paylaşmak istiyorum, çünkü Meclis çatısı altında iki çalışmadan bahsetmek belki buradaki arkadaşların da bilgilenmesi anlamında önemli. Bir tanesi, geçtiğimiz dönem içerisinde Meclis içinde bir Bilişim ve İnternet Araştırma Komisyonu kuruldu ve bu Komisyon çalışmalarını tamamladı.1140 sayfalık bir rapor hazırlandı ve bu raporun neticesinde de 158 tane önerimiz oldu. Ben de bu Komisyon içerisinde Erdal Bey'le birlikte görev yapan milletvekillerinden birisiyim. Buradaki önerilerimizin en başında, tabii, Anayasa içerisinde İnternet'in bir hak olduğu ve bununla alakalı bazı görüşler birinci sırada yer alırken, ikinci sırada bir bilişim bakanlığı kurulmasıydı. Bu sunum içerisinde de bahsi geçen yani bu tür işlerin bir merkezde toplanması ve hatta belki de bir Başbakan Yardımcılığı şeklinde bu işin koordine, diğer bakanlıkların koordine edilebilmesi anlamında önemine binaen böyle bir görüş oluştu. Eğer, tabii bu söz konusu olmazsa bilişim ajansı veya o da söz konusu olmazsa gerek Ulaştırma Bakanlığı gerekse Bilim Sanayi Bakanlığının yeniden yapılanmasıyla alakalı bazı tavsiyeler, öneriler de burada oldu. Ben, özellikle bu öneriler kısmını Komisyondaki arkadaşlarımıza dağıtılmasının faydalı olacağını düşünüyorum.

Diğer taraftan, Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonu içerisinde de gene geçtiğimiz yıl içerisinde elektronik ticaret ile istenmeyen elektronik postalar ve istenmeyen kısa mesajlarla alakalı bir kanun çalışmamız oldu, tamamlandı, Genel Kurula gelmek için sırada bekliyor. Burada da Komisyon olarak oy birliğiyle, hem ticaretin denetlenmesi hem de özellikle bu istenmeyen e-postalar ve mesajların belli bir çerçeveye bağlanması anlamında bir çalışma gerçekleşti.

Şimdi, bütün bunların neticesinde, aslında şöyle bir çıkarımda da bulunabiliriz. Yani, bizim özellikle suçlar anlamında gerek ihtisas mahkemeleri, hâkimler, savcılar, hatta hukuk fakültelerinde bu konuda özel bölümler oluşturmaya kadar geniş bir alanı aslında şu anda incelediğimizi söyleyebiliriz. Dolayısıyla, ben buradan yani şöyle bir şey olabilir mi diye paylaşmak istiyorum: İşin teknik tarafında oldukça detaylı bir çalışmayı Hocam bizimle paylaştı, aynı çalışmayı hukukçuların da olduğu ortamda aslında genişletirsek bence çok faydalı bir iş yapmış oluruz yani Hocamın bu sunumunu. Bahsettiğim gibi, gene üniversitenin hukuk alanlarında bu konularda uzman olan kişilerle birleştirerek bir çalışma ortamı oluşturursak -biz de Komisyon olarak- oldukça faydalı olacağı kanaatindeyim.

Hocam bir de "Demo yapıldı." dediniz birkaç sefer. Aslında böyle fiziksel bir demo yapılmadı yani pratik anlamda bir şey yapılmadı. Dolayısıyla, belki bütün Komisyondaki arkadaşların meraklarının giderilmesi anlamında böyle bir demo da bize ciddi manada fayda sağlayabilir.

Teşekkür ediyorum.

BAŞKAN – Teşekkür ederim.

Sayın Erdem…

ENVER ERDEM (Elâzığ) – Teşekkür ederim Sayın Başkanım.

Ben de değerli Hocamıza vermiş olduğu bilgilerden dolayı teşekkür ediyorum. Ancak, değerli Hocamız bu İnternet, bilgisayar, cep telefonları, casus yazılımlar, akıllı telefonlarla ilgili özellikle bunlar üzerinden yapılacak haberleşme ve bunlar üzerinden yapılan görüşmelerdeki bilginin güvenliği nasıl sağlanabilir ve ne tür eksiklikler vardır noktasında çok önemli bilgiler verdi. Kendilerine teşekkür ediyorum.

Ancak, çok kısa olarak, özellikle, haberleşme hürriyetinin ihlal edildiği, bu dinleme olaylarıyla ilgili olarak yani herhangi bir araçla dışarıdan bir ortam dinlemesi şeklinde, bu haberleşme hürriyeti veya özel hayatın gizliliğini ilgilendiren alanlarla ilgili olarak, özellikle BTK'nın sorumlu olduğu bu frekans tahsisleriyle ilgili hususta, BTK'nın görevini bu anlamda yapmadığına yönelik ciddi değerlendirmeler ve eleştiriler mevcuttur. Maalesef, BTK'nın bu temel sorumluluğunu bizim de şu ana kadar tespit edememizden kaynaklanan, bize her ne kadar TİP'ten bilgilendirme noktasında bir destekleri olduysa da temelde bu frekans tahsisleriyle ve denetimleriyle alakalı noktada bir açıklama yapmadılar. Ben, değerli Hocamıza özet olarak şunu sormak istiyorum: Bu frekans tahsisleri -yani diğer bir ismiyle "Spektrum" falan mı deniyor- işte şu aralıklarda tahsis ediliyor. Bu tahsis edilen frekansların BTK tarafından ne kadar denetlenip denetlenmediğini veyahut da teknik olarak denetlemenin yüzde 100 mümkün olup olamayacağıyla alakalı bir bilgi sunarsanız, bence, Komisyona faydalı olur. Çünkü, en büyük ihlallerden birisi, nihayetinde devletin elinde olan bu frekansları tahsis etme yetkisi ve bunu takip edecek olan kurumun görevini yapmasıyla da alakalı bir boyutu var. Yani, bu kurumun bu görevini tam olarak yapmadığını düşünüyorum veyahut da bu alanda değerlendirmeler var. Hocamız da bu konuya bir açıklık getirebilirse yani bu frekans tahsislerinin denetimi…Çünkü, dışarıdan bu frekanslara herhangi bir şekilde müdahale edildiği zaman, bunu devletin denetim biriminin görmesi gerekiyor. Bunların mümkün olup olamayacağını veya yapılıp yapılmadığına ilişkin sizin bilgilerinizi ben rica ediyorum.

Teşekkür ederim.

BAŞKAN – Teşekkür ederim.

Sayın Alpay…

ŞUAY ALPAY (Elâzığ) – Ben de sunum için çok teşekkür ediyorum. Gerçekten istifade ettiğimizi düşünüyorum.

Sunumunuz sırasında, devletin ve istihbarat faaliyetini yapan kurumlar dışında da yasa dışı dinleme ve izlemeyi yapan şeylerin olduğunu ve olabileceğini ifade ettiniz.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Kesinlikle.

ŞUAY ALPAY (Elâzığ) – Bu konuda çok somut olarak sormak istiyorum: Devletle ilgili olarak bildiğimiz gibi şu anda resmî olarak dinleme yapan MİT var, jandarma istihbarat var, emniyet istihbarat var, Genelkurmayın "GES" komutanlığının devre dışı kaldığı söyleniyor ama o da tartışmalı. Dinlemeye devam edildiğine dair kanaatler ve tereddütler de var. Bu bahse konu kurumlar dışında, size göre yerli ya da yabancı olarak bu yasa dışı dinleme ve izleme faaliyetleri hâlihazırda hangi tür oluşumlar tarafından yapılıyor? Bu konuda üniversitelerin akademik çalışma olarak merak saikıyla yaptığı bir hazırlık ve çalışma var mıdır? Yöntem olarak hangi yöntemler kullanılıyor? Özellikle, bu mobil cihazlar kullanmak suretiyle ortam dinlemeleri burada daha çok dikkate değer olarak duruyor, özellikle yasa dışı dinleme, izleme ve özel hayatın gizliliğinin ihlalleriyle ilgili olarak. Bu konuda, deminden beri anlattığınız sistem içerisinde bir karar verilse, dense ki "Şu anda üniversitelerle acil modda bir iş birliği yapalım ve yasa dışı dinleme ve izlemeleri tespit edelim." bu hemen tespit edilebilecek somut bir vaka olarak duruyor mu, yoksa uzun bir inceleme ve hazırlık mı yapmak gerekir?

Bir de bu millî yazılım önemli elbette, biz de katılıyoruz. Millî yazılımla birlikte ülke içerisinde -milletten kastımız da, ülke içerisinde yani yerele ait olan, bize ait olan unsurların devreye girmesinden bahsediyoruz- bu yasa dışı dinleme ve izlemelere engel olmak açısından… İşte, Iphone bize ait olan bir şey değil ve bunlar üzerinden yapılan işletim sistemleri, yazılımlar ve üstündeki donanımlar bütün bu rezilliklerin ortaya çıkması için de araç olarak kullanılıyor, bunun da fakındayız. Sunumunuz zaten buna dair çok önemli şeyler ortaya koydu. Türkiye'de gerek cep telefonu gerek başka tür cihazları millîlik esası üzerine –tırnak içerisinde söylüyorum- yaparsak, bunlara engel olma imkânı var mı, yoksa uluslararası ticari oluşumlarda bu konuda devrede olduğu hâlde bundan çok emin olabilir miyiz?

Teşekkür ederim.

BAŞKAN – Teşekkür ederim.

Hocam, tabii not alma imkânınız olmadığının farkındayız. Bizim, bunların hepsi de tutanaklara geçti. Global olarak şu an değerlendirme yapabileceğiniz hususlar varsa bunları değerlendirin, bilahare, tutanakları arkadaşlar size iletir, değerlendiremediğiniz hususları yazılı olarak Komisyona gönderirseniz biz arkadaşlara dağıtırız.

Buyurun.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Teşekkür ederim Sayın Başkanım.

Şimdi, ülkede hakikaten pek çok konuda problem var. Bu sorduğunuz sorular aslında sadece burada değil, dünyanın gündeminde olan sorular ve cevap bekleyen sorular.

Şimdi, bu tür sorulara cevap verecek Türkiye'deki üniversitelerde bir altyapılanma henüz yok yani bu konulara kafa yoran hoca sayımız çok yok maalesef. Yani, gördüğüm şeyi söylüyorum ama bunlar için çalışma gerekiyor, araştırma gerekiyor, rapor gerekiyor, destek gerekiyor. Şimdi, "millî yazılım" dediğimizde şöyle sanki geliştirelim de ülkede kullanalım gibi öyle bir şey söylemiyorum. Söylemek istediğim şey şu: Siz yazılımlarınızı geliştirirseniz teknolojiyi bilirsiniz, açıklarını bilirsiniz, nerede problem var farkında olursunuz. Geliştirmediğiniz sürece, o bilgi seviyesine çıkmadığınız sürece, sunulan yazılımlarda ne açıklar var onun farkında olamayabiliriz. Bugün, cep telefonu üretiliyor mu? Evet, Türkiye'de bir cep telefonu üretilecekti, rantabl bulunmadı, gitti. Ama, devlet de o zaman destek verebilirdi, cep telefonları belki bu kadar bir Iphone olmazdı ama Iphone benzer şu anda teknoloji üretebiliriz diye düşünüyorum. Çünkü, çoğu teknoloji de Çin'de üretilip... Donanım geliyor ama yazılım üretiyorsunuz. Cihazların içerisinde şu anda yazılım var, hepsi yazılım.

ENVER ERDEM (Elâzığ) – Hocam, yazılımla ilgili durumuz ne? Yani, bizim yazılım mühendisi sayımız yeterli mi?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Evet, şimdi, Türkiye'de yazılım mühendisliğiyle ilgili bölümler var, şu anda bildiğim kadarıyla beş üniversitede yazılım mühendisliği bölümü var, yeni açılanlar da var. Yani bu yönde eleman yeterli midir? Çok yeterli olmadığını düşünüyorum, olsa biliriz. Şimdi, yazılım işi önemli bir iş. Ne açıdan? Artık bir mühendislik, o mühendislik bakış açısıyla yazılımları geliştirmek zorundasınız. Mesela, biz, Iphone'a bir uygulama geliştirdik, Iphone reddetti uygulamamızı geçen hafta. Çünkü, "Bizim bir standardımız var, o standarda uygun değil." dedi. Böyle de bir prosedürleri var. Iphone ticari bir şirket ve bu endişeleri herkes onlara aktarıyor. Yani, Iphone bunları yapıyor gibi bir şey yok, engellemeye çalışan en ciddi firma. Çünkü, Iphone, onun için Apple Store'u kurdu, onun için pek çok şeyi sınırlı indiriyorsunuz. Onlar testlerden geçiyor, pek çok uygulamayı oraya koymuyor. Yani, öyle de düşünün, milyar dolarlık, trilyon dolarlık bir şirket riske atmaz kendisini ama ihlal olabilir mi? Olabilir, her şeyde olduğu gibi ama Apple mantığını iyi anlamak gerekiyor, mükemmeliyetçi zihniyeti iyi anlamak gerekiyor. Bir iş yaparken o kadar geniş kapsamlı düşünmemiz gerektiğini bize ifade ediyor. Yani, burada üniversitelerde yapılması gerekenler, üniversiteler bu konuya daha çok önem vermeli. İşte, bizim ders teklifimiz var -sayın vekilimin sorduğu- üniversitelerde eğitim verilmeli. İşte, kişisel verilerin korunması, bilgi güvenliği, teknolojinin verimli kullanılmasına yönelik dersler verilmeli. Hoş, şu anda "enformatik" diye bir dersimiz var üniversitelerde ama içinde Word, Excel, Powerpoint öğretiyoruz, ben bildim bileli bunu öğretiyoruz. Biz de kaldırdık kendi bölümümüzden, bölüm başkanı olduğum zaman, bu dersi kaldırdık yerine bilgisayar mühendisliğine giriş dersi koyarak, bu tür dersleri destekledik. İşte, bölümümüzde, kendi bölümümüzde, şu anda bilgi güvenliğiyle ilgili en fazla ders açılan bölümlerden birisiyiz Türkiye'de. Bu farkındalığımızı hem STK tarafında sürdürüyoruz hem üniversite tarafında ama yeterli mi? Tabii, çalışmak gerekiyor, bu işin arkasında o var. Kafa yormak

gerekiyor, üretmek geriyor. Ürettiğimiz çok güzel şeyler de var. Mesela, bu çalışmalarımızdan, parmak izinden yüz eşkâli belirleme, parmak izinden cinsiyet belirlemeyle ilgili dünyada ilk çalışmaları yaptık ve bunu basınla da paylaştık. Bakın, kişinin parmak izinden cinsiyetini otomatik belirleyen sistem tasarladık, patentlerimiz var bu konuda, projeler yapıyoruz. Mesela, ülkede neler yeterli değil? Bu da lütfen özellikle kayıtlara girsin. Şimdi, biyometrik alanında parmak iziyle ben çalışmak zorundayım ki bu geliştirdiğim sistemleri dünyaya pazarlayabileyim ama ben veri alamıyorum çünkü kanun diyor ki "alamazsınız" üniversitelerle veri paylaşılmıyor, neden biz AR-GE yapamıyoruz. Şu anda ben yurt dışından veri satın alıyorum, o da çok sınırlı. Ama yine…

HASİP KAPLAN (Şırnak) – Hocam, neden AR-GE yapamıyorsunuz?

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Şöyle, yapamadığımız şey, verimiz yok elimizde bakın. Ülkede AR-GE'ye açılacak veriye ihtiyaç var ki analiz edelim. Mesela, bu ülke trafiğinin bir kısmını bize sunsunlar, analiz yapalım, oradan sonuç çıkartalım. Hep sentetik veri üretiyoruz, sentetik verilerle çözüm bulmaya çalışıyoruz. Ama benim elimde parmak izi olsa, benim elimde yüz verileri olsa, ben oradan çok farklı çalışmalar yapabilirim. Ama bunu "Kanunda var." diye kurumlar paylaşmıyor, paylaşmadığı için de çalışmalar, maalesef, belli bir noktaya erişmiyor.

Pakistan'dan teklif alıyorum, başka ülkelerden teklif alıyorum, "Gelin Hocam, ekibinizle burada çalışın." diye, ama burada çalışamıyorum, neden? "Veri verilemez." deniyor. Mesela, bu yönde bu tür çalışmaların yapılması için üniversitelere biraz özerklik tanınmalı, kişilerin mahremiyetlerini, gizliliğini korumak kaydıyla tabii ki, o hassasiyeti belirlemek kaydıyla, o hassasiyet çerçevesinde. Ama biz AR-GE'yi neyle yapacağız? Veriyle yapmak zorundayım. Verisiz AR-GE yok. Mesela bu konuda en dertli hocalardan birisiyim. Bunu TÜBİTAK Başkan Yardımcımıza aktardım, çok olumlu baktı "Hocam, çok haklısınız." dedi. Şu anda proje teklifleri var, bunu verin, ülkede açık kaynak bir veri havuzu oluşturalım, bütün araştırmacılar oradan veri alsın, çalışsın, ülkeye katma değer oluşsun… İşte o noktadayız şu anda.

BAŞKAN – Yani ülkemiz, kişisel verilerin korunması anlamında, veri güvenliği anlamında diğer dünya ülkelerine göre daha mı ketum, daha mı...

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU - Yo, o yönden söylemedim, ketumluk değil de… Evet, kanunlar çok sert. AR-GE konusunda veremiyorlar çünkü kanun maddesini getiriyor oradaki arkadaşlarımız, başkanlarımız, müdürlerimiz, "ketum" konusunu…

BAŞKAN – Yani biz koruma altında...

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Yo, uyguluyorlar, tabii ki uyguluyorlar.

Mesela ben bir araştırmacı olarak alamadım, herhâlde, en son Sayın Başbakanımıza gideceğiz, böyle özel bir kanun çıkması için. Çünkü biz AR-GE yapmak istiyoruz. Dünyada ses getiren ARGE yapıyoruz. Ama bunu belirli noktada işte 700 veriyle test edebiliyoruz çünkü ben öğrencilerimden topluyorum bu verileri, o kadar. Ama yüksek veri tabanlarıyla bunu test etsem…

Bakın, Japonya'ya bile gittim veri alabilmek için, inanın paylaşmıyorlar. "Japon üniversiteleriyle iş birliği yapalım." dedik, doğru yapıyoruz, ama her şeyi sorguluyor, ülkeye gelmesini istemiyorlar. Biometrik konusunda çok ilerideler. Böyle bir ketumluk her ülkede var, biometrik veri hassas bir veri. Ama "bu paranoyaları tetiklemeyelim" diye, biraz önce konuşuldu ya, "şimdi parmak izlerimiz alınıyor, bilmem ne yapılıyor" gibi gündemi de meşgul etmemek gerekiyor. Bu paranoya, zaten, herkesi germiş durumda, kurumlarda hassasiyet had safhada. Yani, ben, hiçbir şekilde veri alamadım bu konuda. Ama olmak zorunda. Sentetik isimler, resimler farklı olabilir. İfşa edilmeden bunlar testlerde kullanılabilir. Ha, tabii, teknoloji üretmek istiyorsak, tabii kişisel verilerin korunması önemli. Biraz önceki bu anlattığım sunumda da dikkat edilmesi gereken husus bu yani anlatılanlardan çok korktuk, her şeyi keselim… Hayır, açalım ama denetim şeffaflığını da açalım, beraberinde getirelim. AR-GE'yi yapalım, bizler yapacağız. Genç nüfusu olan bizleriz. İnanın gençlerimiz pırlanta. Yaptıkları projeleri ben size anlatsam… Gidip Amerikalarda sunuyoruz, burada sunamıyoruz.

Bakın, youtube'da yüklenen videolar içerisinde gizli bilgi var mı yok mu, bununla ilgili çalışma yapıyor çocuklarımız. Oraya gidiyoruz, orada dinleniyor, biz burada… Veri gerekiyor, veriyle ancak çalışma yapılır. Veriyi nereden bulursanız oraya yöneliyorsunuz.

BAŞKAN – Evet, teşekkür ederiz Hocam.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Biz böyle dertliyiz, çok dertli bir alana girdik ama…

BAŞKAN – Siz, yine, tutanaklardan soruları arkadaşlar size gönderirler, detaylı yazı hem daha sağlıklı olur.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Tabii, tabii çok doğru.

BAŞKAN – Biz, tabii ki davetimizi kabul ettiğiniz, Komisyonumuza sunum yaptığınız için Komisyonumuz adına teşekkür ediyoruz.

GAZİ ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ PROF. DR. ŞEREF SAĞIROĞLU – Ben teşekkür ederim davet ettiğiniz için, faydalı olur inşallah, sağ olun.

BAŞKAN – Rica ederiz.

Evet, değerli arkadaşlar, bugünkü gündemimiz tamamlandı.

Yarın yine saat 11.00'de bu salonda toplantımızı yapacağız.

Bugünkü toplantımız sona ermiştir, toplantıyı kapatıyorum, hepinize iyi günler diliyorum.

Kapanma Saati: 13.05