



ANKARA ŞUBESİ

BİLGİ GÜVENLİĞİ VE GÜVENİLİR BİLGİ PANELİ E-KİTAP



10 Nisan 2014 - Ankara

ISBN:978-605-01-0680-0



“BİLGİ GÜVENLİĞİ VE GÜVENİLİR BİLGİ”

PANELİ

(10 NİSAN 2014)

1. Baskı, Ankara-Ocak 2015
ISBN:978-605-01-0680-0
EMO Yayın No: EK/2015/589

TMMOB Elektrik Mühendisleri Odası Ankara Şubesi
İhlamur Sokak No:10 Kat:2 06640 Kızılay Ankara
Tel: (312) 231 44 74
Faks: (312) 232 10 88
<http://www.ankara.emo.org.tr>
E-Posta: ankara@emo.org.tr

Dizgi

TMMOB Elektrik Mühendisleri Odası Ankara Şubesi



Sunuş

10 Nisan 2007 tarihinde aramızdan ayrılan EMO Ankara Şubesi 6. ve 7. Dönem Yönetim Kurulu Üyesi Halil Eker anısına 10 Nisan 2014 tarihinde “Bilgi Güvenliği ve Güvenilir Bilgi” paneli EMO Merkez Toplantı Salonu’nda düzenlendi.

Panelde konuşmacı olarak İ. İzlem GÖZÜKELEŞ (Bilgisayar Mühendisi), Av. Yelda Gizem ÜNAL (Ankara Barosu Elektronik Haberleşme Hukuku Kurulu Başkanı), Engür PİŞİRİCİ (Bağımsız Siber Güvenlik Araştırmacısı) yer aldı.

“Bilgi” ve “veri” sözcükleri zaman bağlamında etimolojik olarak hiyerarşik (data, information, knowledge) bir ilişkiyi barındırmaktadır. Fakat Türkçe’ye çevrilirken sınırlı kavramlarla ifade edilmiştir. “Data” dün’e, “information” bugün’e, knowledge ise yarın’a ait bir bilgidir.

İnternet kapitalizm açısından 1990’lı yıllardan itibaren yeni bir sermaye birikim modeli olarak değerlendirilmeye başlanmıştır. Elektronik ticaret ve iletişim başta olmak üzere bilgi (information/ knowledge) toplumu olma yönündeki gelişmeler dünya üzerindeki tüm ülkelerin mevcut yapısını değiştirmiş ve yeniden şekillendirmiştir. Bu değişim ülkemize ancak 2000’li yıllarda gelmiştir.

Bilgilerin izinsiz kullanımını, izinsiz erişimini, ifşa edilmesini, yok edilmesini, hasar verilmesini, değiştirilmesini önlemek için yapılan tüm koruma çabaları bilgi güvenliği başlığı altında toplanmakta; bilgi güvenliğinde amaç doğru teknolojilerin kullanılmasıyla bilgiye izinsiz tüm erişimleri engellemek olarak görülmektedir.

Bilgi teknolojilerinin yaygınlaşmasıyla bilgi teknolojilerini kullanarak yapılan elektronik müfahaleler hızla artmaktadır. Sayısal bilgilerin gizlilik, bütünlük ve erişilebilirlik riskleri arttığında bilgi güvenliğinde ciddi sıkıntılar yaşanabilmektedir.

Bilgi ve veri kim için, nasıl kullanılacak? Bu soruya verilecek yanıt bilgi güvenliği konusunda nasıl bir yöntem izleneceği sorusuna doğru yaklaşmak bakımından önem taşımaktadır. Reyhanlı saldırısının ardından askeri istihbarat belgelerini yayımlayan, YÖK’ün belgelerini yayımlayarak üniversitelerdeki yolsuzluk ve usulsüzlükleri ifşa eden, Ankara Büyükşehir Belediye Başkanı ile ilgili belgeleri yayımlayan, Gezi direnişi sırasındaki tutumları nedeniyle perk çok kamu kurumu



ve kuruluşunun web sayfalarını hizmet dışı bırakan redHack grubunun eylemleri ile bilginin kamusal niteliği arasındaki diyalektik ilişkiyi anlayabilmek önemlidir. Benzer şekilde Wikileaks'te yayımlanan belgelerin dünyada üstü örtülmeye çalışan birçok olayı tüm gerçekliğiyle açıklamış ve hakikate erişimde cesur ve önemli bir adım olarak tarihe not düşülmüştür.

Öte yandan iktidar sahipleri kamu olanakları sayesinde dönemsel veya asıl tehdit olarak gördüğü unsurların bilgisayarlarına sızarak, sahte belgeler düzenleyerek “delil” üretmektedir. Son dönemdeki Türkiye tarihinde iz bırakan Ergenekon ve Balyoz davalarında dijital delillerin bu yollarla üretildiği bilirkişi raporları ile kanıtlanmıştır. Bu durum da bilgi güvenliğinin insanların temel özgürlüklerinin, düşünce ve ifade özgürlüklerinin önünde ne gibi sonuçlar yol açacağı bağlamında ibretliktir.

Tüm bunları ve daha fazlasını tartışıp Odamızın bilgi güvenliği konusundaki dağarcığını geliştirmek adına düzenlediğimiz bu etkinliğin kayıtlarını başta üyelerimiz olmak üzere tüm kamuoyu ile paylaşıyoruz. Etkinliğe katılan, sunum yapan, destek veren tüm taraflara teşekkürlerimizi sunuyoruz.

Saygılarımızla.

EMO Ankara Şubesi

22. Dönem Yönetim Kurulu



OTURUM BAŞKANI (Ebru Akgün Yalçın)- Sevgili dostlar, değerli meslektaşlarımız, Halil Eker'in değerli dava arkadaşları; hepiniz hoş geldiniz.

Bildiğiniz gibi, Halil Eker'i kaybedeli 7 yıl oldu, 10 Nisan 2007'de kaybettik kendisini.

Halil Eker, 18. dönem Odamız Yönetim Kurulu üyeliği yapmış, 19, 20 ve 24. döneme kadar Odamız Onur Kurulu üyeliklerinde bulunmuş, arkasından 6. ve 7. dönemlerde Şube Yönetim Kurulu üyemiz olarak görev yapmış bir ağabeyimiz; ülkenin üzerine karabasan gibi çöken 80'li yıllarda, bu zor görevi mücadele arkadaşlarıyla birlikte göğüslemiş, Odamızın birçok kurulunda görev almış bir büyüğümüzdür. Kendisinin yokluğu, aslında anmalarımızda ifade ettiğimiz gibi, her geçen gün bizi etkiliyor. Bugün mezarlık anmasını da eşiyle ve arkadaşlarıyla birlikte yapmıştık; anısı her daim bize yol gösterecektir. Onların o zorlu dönemlerde mücadele adına yapmış oldukları, Odamızın 60 yıllık geçmişine döşedikleri tuğlalar hâlâ buralarda, bu binanın tuğlaları onların elinden geçmiş durumda. Hepsini saygıyla anıyoruz.

Halil Ağabey özelinde, demokrasi mücadelesinde yitirdiğimiz tüm değerlerimiz adına sizleri 1 dakikalık saygı duruşuna davet ediyorum.

OTURUM BAŞKANI- Anıları mücadelemize ışık tutacak.

Halil Ağabeyi geçmiş günlerden anmak adına ufak bir Powerpoint sunumumuz vardı, onu izleyelim.

OTURUM BAŞKANI- Halil Ağabeyle ilgili duygu ve düşüncelerini paylaşmak isteyen var mı?



Gülcan Abla, siz bir şeyler söylemek ister misiniz?

Buyurun.

GÜLCAN EKER- Arkadaşlar; buraya kadar geldiğiniz için hepinize teşekkür ediyorum, hoş geldiniz diyorum.

Fazla konuşmayı beceremem, çünkü bizde hep Halil konuşurdu. Aramızdan ayrılalı 7 yıl oldu; kolay yıllar değildi bunlar, zor yıllardı. Ancak her şeye rağmen hayat devam ediyor; çoluk çocuk, ev işi, torun derken vakit geçirmeye çalışıyoruz.

Halil çok mücadeleci bir insandı; Oda için çok fazla çalıştı, çabaladı, emek verdi. Gençlerin Odaya sahip çıktığını görüyorum, bu da beni sevindiriyor, onun emeklerinin boşa gitmediğini anlıyorum. O zamanki mücadele çok farklıydı, şimdiki mücadele çok farklı, ama dediğim gibi, ne şekilde olursa olsun, hayat devam ediyor. Hastalık onu bizden erken ayırdı aslında, yaşı çok fazla değildi. Her şeyde mücadele ederken, hastalıkta da çok mücadele etti, ama orada başarılı olamadı, maalesef 7 yıl önce bizleri ve sizleri bırakıp gitti. Bunun yanında, Ahmet Ağabey, Güney Hoca, dayım Baki Uzel -belki tanırıyorsunuz, belki tanımazsınız, o da elektrik mühendisiydi, onu da bir trafik kazasında kaybettik- hepsine rahmet, geride kalanlara da sağlıklı, sıhhatli ömürler diliyorum.

Tekrar hoş geldiniz. Teşekkür ediyorum.

OTURUM BAŞKANI- Başka söz almak isteyen?

Bugün mezarlık anmasında Niyazi Bey de bizlerleydi. Kendisi, gün ve ay olarak da ilk tanıştıkları günü anlatmıştı. Ankara'ya iş için ilk geldiğinde -Maçka'dan geliyorlar- Halil Bey'e telefon ediyor bir arkadaşı, "*Halil, gel buraya; senin gibi komünist birisi geldi, tanıştırayım sizi*" falan diye. O gün tanışıyorlar ve ondan sonra zaten 45 yıl boyunca bilfiil beraber oluyorlar. Niyazi Bey mezarlıktaydı, ama "*Akşam herhalde gelemem*" dedi.



GÜLCAN EKER- Telefonda konuştuk, gelecekler.

OTURUM BAŞKANI- O zaman geç mi kaldılar?

GÜLCAN EKER- Biraz yorulmuşlar, “*dinlenelim*” dediler. “*Çıktık*” diye telefon açtılar, ama trafikten dolayı biraz geciktiler herhalde.

OTURUM BAŞKANI- O zaman şöyle yapalım: Biz bu kaybettiğimiz büyüklerimizi anmak adına, aslında onların isimlerini de ölümsüzleştirmek ve aynı zamanda ahde vefa borcu olarak, gündeme



ilişkin olarak, yani o dönemin ihtiyacına ilişkin olarak bazı etkinlikler yapıyoruz. Bugüne yönelik olarak da “*Bilgi Güvenliği ve Güvenilir Bilgi*” başlığında bir panel yapmak istedik. Son dönemde bilginin ne olduğu konusunda; gerçek, doğru, güvenilir bilgi üzerinde aslında çok fazla spekülasyon oldu, oluyor ve her daim olacak şeyler bunlar. Ancak özellikle Gezi sürecinden sonra başlayan ve sosyal medya üzerinden bilginin paylaşımının farklı mecralarda sürüklendiği ve ilerlediği gerçeğinden bakarak, bugüne ilişkin bir şeyler söyleme ihtiyacı hissettik açıkçası.



17 Aralık operasyonlarının arkasından çıkan tape'lerden tutun da hemen yanı başımızda Twitter, Youtube yasaklarına baktığımız zaman, bu bilgiye yönelik olarak aslında “Bizlerin ulaşabileceği nedir, bizlere sunulan nedir?” üzerinden bir tartışma yürütelim istedik. Youtube en son kapalıydı, açıldı mı bilmiyorum; dün açıldı, bugün tekrar kapandı, hâlâ kapalı. Böylesi bir dönemden geçiyoruz.

Çok değerli konuklarımız olacak, ben onları davet etmek istiyorum: İzlem Gözükeleş, bilgisayar mühendisi. Yelda Gizem Ünal,

Ankara Barosu Elektronik Haberleşme

Hukuku Başkanı. Engür Pişirici, bağımsız siber güvenlik araştırmacısı.

Panelin kurgusunu ifade edeyim isterseniz: Konuşmacılarımıza 20'şer dakikalık bir süre vereceğiz, onlar çerçeve sunumlarını yapacaklar. Sonra salondan katkı ve sorular alacağız. Arkasından tekrar kendilerine hem toparlamak hem cevap vermek adına 5'er-10'ar dakika yeniden söz vereceğiz. Ortalama 2 saat gibi bir süremiz var sanıyorum. Gerçi mekân bizim, onunla ilgili herhangi bir sıkıntımız yok; sadece akşam saati, sizlerin tahammülünü zorlamamak adına...

İlk sözü bilgisayar mühendisi arkadaşımız İzlem'e veriyoruz.

Buyurun.

İZLEM GÖZÜKELEŞ (Bilgisayar Mühendisi)- Teşekkür ederim.

Gözetim hakkında konuşmak istiyorum. Gözetimden, özel hayattan





bahsetmeye kalktığımızda, iki farklı yaklaşım var, aslında ikisi de aynı bence: Birincisi, Hakan Şükür'ün yaklaşımı, bu yaklaşım ülkemizde çok yaygın. Hakan Şükür şöyle diyor: *“Hepimizin telefonları dinleniyor olabilir. Düzgün bir duruşunuz ve yaşam biçiminiz varsa, o telefon dinlemesi sizi rahatsız etmez; beni rahatsız etmiyor.”* Hatta 2008 yılında kanun değişmişti, polise isteyen vatandaşlardan parmak izi alma yetkisi verilmişti. Trabzon polisi stant açıyor, insanlar koşa koşa parmak izi veriyorlar. *“Neden böyle bir şey yaptınız?”* diye soruyor gazeteci; *“Benim korkacak bir şeyim yok ki, ben çok iyi vatandaşım, çok iyi bir Türk’üm”* vesaire... İkincisi, bizim klasik aktivistlerin, muhaliflerin tavrı; *“Ben çoktan fişlenmişim, derin devlet zaten benim her şeyimi biliyor, ne olacak ki?”* O yüzden bu aktivist arkadaşlarımız, Facebook’u, Twitter’ı gönül rahatlığıyla kullanıyorlar. Bakalım başlarına neler gelecek...

2011 yılında bir gazetede bir haber yayımlandı; şöyle diyordu: *“Devrimler önceden tahmin edilebilir.”* Buradaki devrim sözüne takılmayın; devrimleri tahmin etmek derken Leetaru adlı yazarın *“Arap baharındaki ayaklanmalar, aslında önceden bilinebilirdi”* tezinden bahsediliyordu. *“Bu adam bunu neye dayanarak söylüyor?”* diye araştırdığımda, şöyle bir şeyle karşılaştım: *Culturomics* denilen bir bilim dalı var, sayısal sözcük bilimi. Kitapların sayısallaştırılmasından ve arşivler üzerinden insan davranışlarını ve kültürel eğilimini inceleyebiliyorlar. Şöyle ki: Google, bayağı bir kitabı sayısallaştırdı. Bu kitaplar içinde geçen bazı kelimelere bakarak ya da dilin kullanımına bakarak, o dönemin insanları neler düşünüyordu, eğilim ne yönde gelişti, görebiliyorlar. Mesela “yabancılaşma” kelimesini arattığınızda, yabancılaşmanın 68 sonrasında, 80’e kadar çok gündemde olduğunu, 80’den sonra düşüşe geçtiğini görebiliyoruz.

Aslında bu yeni bir şey değildi. Geçmişte ABD, Japonlar üzerinde bu yöntemi kullanıyor. Japon radyolarını sürekli dinleyerek, Japon kamuoyunun kendilerine olan tepkisini anlamaya çalışıyorlar. Radyodaki haberlerde ton biraz nefrete doğru gidiyorsa, *“Savaş çıkma*



ihhtimali var” gibi yorumlar yapmışlar. Mesela Türkiye’de de gazetelere bakarsanız, hangi ülkeyle aramızın iyi olduğu, hangisinin kötü olduğunu dönemsel olarak görebiliriz. Mesela İran’la yakınlaştığımız dönemlerde, İran’la ilgili haberler artacaktır; başka ülkeyle yakınlaşırsak, onunla ilgili olumlu haberleri artacak. Kimi zaman düşmanınız Suriye olacak, Suriye yerin dibine geçecek.

Leetaru, analiz yaparken şöyle diyor: *“Kitaplar sadece geçmişe yönelik bilgi verir. Ben eğer güncel haberleri araştırırsam, oradaki kelimenin tonuna -öfke, övgü, sövgü vesaire- bakarsam, oradaki durumu da anlayabilirim.”* Bunu Mısır üzerinde deniyor. Burada 100 milyondan fazla makaleyi inceliyor ve bu makalelerdeki bazı kelimelerin -öfkeyi, sevinci vesaire belirten kelimeler var- tonuna bakarak havanın değişimini sezebileceğimizi söylüyor. 100 milyon makale üzerinde yaptığı araştırmada, mesela 91 yılında Mısır’da olumsuzluğun en alt seviyeye indiğini görüyoruz; çünkü 91 yılında Körfez Savaşı var. Aynı durum Ocak 2011’de de gerçekleşmiş; bundan sonra zaten Mübarek devrildi...

Benzer çalışmayı Tunus’ta yapıyor Leetaru, Tunus’ta da yine aynı bilgiye erişiyor. Aynı şeyi Libya’da yapıyor, Libya’da da benzer bilgiye erişince, *“Tamam, biz devrimleri, aslında ayaklanmaları önceden görebiliriz. Oradaki halktaki olumsuz havayı buradaki haberlerden takip etmemiz mümkün”* diyor. Mesela şu adrese (<https://books.google.com/ngrams/>) bakarsanız, burada Google’ın kitapları var; oradaki kitapların belli kelimelerini aratırsanız -herkesin hakkı var- o eğilimi görebiliyorsunuz. Leetaru, en son şunu diyor: *“Tamam, haberler bize bayağı şey öğretiyor; fakat esas sosyal ağları araştırırsak -‘bu ülkelerde Facebook ve Twitter çok sık kullanılıyordu’- çok daha fazla şey öğrenebiliriz, bazı toplumsal olayları daha çıkmadan önce görme şansına sahip olabiliriz”* diyor.

Burada yeni gözetimden bahsediyoruz. Önceki gözetimde ne vardı? Belli bir kişiye yönelik gözetim vardı, ama şimdi toplumun geneli



gözetleniyor, geneli hakkında bilgi ediniliyor, bu genele dayanılarak bazı sonuçlar çıkarılıyor. Yani devrimler tahmin edilebilir mi; bu konuyu bir yana bırakalım. Ben sadece burada şuna dikkat çekmek istiyorum: Birincisi, burada yeni olan gözetim. Araştırmamanın yöntemini, sonucunu bir kenara bırakalım.

Burada dikkatimizi çeken şey şu: Leetaru'nun araştırması devasa bir veriye dayanıyor. Düşünün, 100 milyondan fazla makale çok kısa

sürede incelenmiş. Ayrıca analiz yapmak için birtakım yollar, veri madenciliği kullanılmış.



Burada neden-sonuç ilişkisi yok. Büyük veri analizi ya da veri madenciliği çalışması yapanlar sadece şunu diyor: *“Veri içinde böyle böyle şeyler gözlemlerseniz, şöyle şöyle durumlar çıkabilir.”* İkisi arasında korelasyon ilişkisi var. Neden olduğunu söylemiyorum size.

Yeni gözetim diyoruz; peki yeni olan ne? Önce gözetimin klasik olanına bakalım: Gözetim, amaçlı bir eylemdir; kontrol etmek, sınıflandırmak, yönetmek, etkide bulunmak gibi amaçlarla yapılır. İkincisi, gözetim rastgele değil, belirli bir plan doğrultusunda gerçekleşir; yüzeysel değil, detaylı bilgiyi hedefler.

Bilgisayar 38-39 yıl önce ilk çıkmaya başladığı zaman, James Rule diye bir sosyal bilimci şöyle diyordu: O zaman herkes *“Big Brother”*ı, *“Bin Dokuz Yüz Seksen Dört”* kitabını konuşuyordu; *“Artık bilgisayarlar ortaya çıktı, hayatımız bitti.”* James Rule buna itiraz ediyor ve yaklaşık 40 yıl önce şunları söylüyor: *“Korkmanıza gerek yok; çünkü kişisel bilgilerin saklanması ve daha sonra bunlardan bilgi kümeleri oluşturabilmek için gerekli teknik ortam yok, bunu teknik olarak*



yapamayız. Farklı yerlerdeki bilgiyi birleştirecek bir sistemimiz yok. Orwell, *Bin Dokuz Yüz Seksen Dört*'ünde bilgisayar sistemleri anlık durumları analiz edip insanlar komutlar veriyorlardı; fakat böyle bir şey olanaksız şu an için." 1984'te bilgisayarlar insanların her anını gözetleyebiliyordu, 70'lerde bu yok. James Rule, "*Tamam, içimiz rahat edebilir*" filan diyor; fakat günümüze bakınca, bunun aslında gerçekleştiğini görüyoruz, teknolojik olarak artık bunlar yapılabiliyor.

Peki, ne değişti? Geleneksel gözetimde şu var: Geleneksel gözetim, şüpheli kişiye yöneliktir; tamam, muhalifler izleniyorsa, devlet nezdinde şüpheli oldukları için. Yeni gözetim ise herkesi kapsar, herkes içinden şüphelileri çıkarır. Geleneksel gözetimde toplanan bilgi yerel mekânda saklanırdı, tek bir yerdeydi; şimdi daha çok üçüncü şahıslarla paylaşılıyor. Bireyler hakkında bilgi toplanırdı önceden; şimdi kitleler üzerine yoğunlaşıyor. Önceden tek bir kaynaktan beslenen bir gözetim vardı; şimdi çok farklı kaynaklar var. Mesela Google'dan, Facebook'tan, Twitter'dan, telefon görüşmelerinden, Skype'tan bir sürü veri akıyor. Toplam veriyi saklamak ve analiz etmek zordu, pahalıydı; şu an çok daha kolay. Veri göndermek ve almak zordu; şu an çok hızlandı. Verilerin birleştirilmesi ve alandaki veri kümeleri oluşması zordu; bugün bu daha kolay. Gerçek zamanlı değildi; bugün gerçek zamanlı veri alabiliyoruz. Daha dar kapsamlı ve yüzeyseldi; şimdi daha geniş ve derinliği artmış veriye sahibiz.

Büyük veriden bahsediyoruz; peki, ne kadar büyük veri? Önceden 1.4 megabyte disket çok büyük veriydi; şimdi 1 terabayt normal. Büyük veriyi tarif ederken 3 V'den faydalanıyorlar. Birincisi veri hacmi (Volume); veri hacmi çok fazla, devasa boyutlarda, her yerden veri akıyor. İkincisi, veri kaynakları ve tipi çeşitli (variety); artık her yerden veri toplanıyor, insan vücudundan tutun da uzay araçlarının hareketine kadar birçok yerden veri toplanıyor ve veri hızla (Velocity) artıyor. Mesela şu anki verinin büyük bir kısmı, son 2-3 yılda toplanan veri ve bu daha da artacak.



Durumu anlatabilmek açısından şöyle bir örnek vereyim: Domuz gribi bir dönem ortaya çıkıyor ve bu gripin nasıl yayıldığını bulamıyorlar. Eğer yayıldığı yeri bulurlarsa ve seyrini tespit ederlerse müdahale edebilecekler, ama bürokrasi falan, bayağı uzun olacak. Bu olaydan birkaç hafta önce Google çalışanlarının bir makalesi yayınlanmış. Google çalışanları şunu diyor: *“Grip salgınını biz önceden görebiliriz. Nasıl? Mesela insanlar günümüzde hasta olunca hemen Google’a başvuruyorlar; ilaç, şifalı bitkiler vesaire...”* Sadece Google’daki aramalardan faydalanarak grip salgınının nereden başlayıp nereye doğru gittiğini tespit etmişler.

Büyük veri sağlıkta kullanılabilir. Mesela erken doğmuş bebekleri kuvüze koydukları zaman, bunların uzun süre gözetimde kalması gerekebilir. Bir enfeksiyon oluşmadan anlamak için, bebekten saniyede bir sürü veri alıyor. Bu verileri anlık analiz ederek bir enfeksiyonu önceden bilebiliyorlar. Yani gerçek zamanda çıksa, 24 saatte ortaya çıkacak; 24 saat önceden anlayabiliyorlar.

Mesela geçtiğimiz yıl PRISM skandalı, Snowden’la başlayan bir skandal ortaya çıktı. Buradaki veri kaynaklarına baktığımızda, şunlar var: Google’daki e-postalar, izlenen videolar, yapılan aramalar, Microsoft ve Apple sistemlerindeki kullanım bilgileri, akıllı telefonlardaki iletişim ve konum bilgileri, Facebook’taki etkinlikler, Skype sohbetleri, bunların hepsi birleşiyor ve ABD hizmetine giriyor. Yani Google’daki e-postalarınızın içeriğini bilecek, her şeyi bilecek.

Büyük veri, geçmişteki araştırmalardan biraz daha farklı. Mesela önce araştırma yaparken teknik sınırlılıklar nedeniyle herkesle görüşemeyeceğimiz için, sadece küçük veri kümeleri oluşturuyorduk ve bu küçük veri üzerinde çalışıp bütüne dair sonuçlara ulaşıyorduk. Mesela bir inşaat yapacaksanız, mühendislik faaliyeti yapacaksanız, ön hesaplarınız birebir aynı olmak zorunda. Fakat büyük veri yaklaşık sonucu tahmin edebiliyor, çok büyük veriden kimi eğilimleri öngörebiliyor. Büyük veri, olgular arasında nedensellik yerine, bağıntı,



korelasyon ilişkisi kuruyor. Yani insanların neden arama yaptığını sorgulamıyoruz, sadece şunu görüyoruz: Arama yapıldığı zaman, bilin ki bir hastalık varmış orada.

Veri günümüzün en önemli şeyi ve her yerden veri akıyor. Mesela şu an NASA'da günde 1 terabyte veri oluşuyor ya da insan genomu projesi, binlerce byte veri kaydediyor. Birçok şirket, müşteri bilgilerini kaydediyor. Kredi kartı işlemleri, telefon kayıtları, Web'deki trafik bilgileri, kapalı devre televizyon kayıtları olağanüstü hacimlerde. Şu an 650 milyondan fazla web sitesi var, 900 milyondan fazla Facebook kullanıcısı ve günde atılan 3 milyar mesaj var. Twitter'ın 150 milyondan fazla kullanıcısı olduğu tahmin ediliyor ve günde ortalama 350 milyon twit atılıyor.

Her yer veri kaynıyor diyoruz; *“Bu veri kaynamasından sonra şöyle bir şey yaptık”* diyor birçok araştırmacı: *“Biz henüz veriden ne yapılacağını bilemiyoruz.”* Bu özellikle 11 Eylül'den sonra daha çok gündeme geliyor. Clinton başta olmak üzere birçok politikacı, araştırmacı şöyle diyor: *“Biz 11 Eylül'ü önceden önleyebilirdik, çünkü elimizde bunun bazı sinyaller vardı. Mesela ABD'ye öğrenci vizesiyle girmiş birinin ticari havacılık kursu alması olağan bir durum değildir. Bu kişinin bazı bilinen teröristlerle dolaylı ilişkisinin olması kuşku uyandırıcıdır. 11 Eylül saldırganlarının 5'inin daha önceden FBI veritabanında vardı zaten. Saldırganlardan biri, 2 yıldır ABD'de olmasına rağmen, 30 kredi kartına sahipti ve elebaşı olarak görülen Muhammed Atta'nın tam 12 tane evi vardı Amerika'da. Biz bunları önceden bilebilirdik.”*

Karşımızda çocukların yaptığı bir şekil var. Bunu ne yapmışlar; rakamları, harfleri sıra sıra birleştirme... ABD'liler şöyle diyorlar: *“Eğer 11 Eylül 2001 öncesinde biz noktaları birleştirmiş olsaydık, şüphelileri yakalayabilirdik.”* Fakat bu o kadar kolay değil. Mesela noktaları birleştirmeye başladığınızda, ortaya çıkan şeklin terörist olduğunu nereden bileceksiniz? Terörist imgesine sahip olmadan,



teröristi nasıl bulacağız? Peki ya saldırı uçakla değil de farklı biçimde ve tamamen farklı araçlarla gerçekleştirilseydi, nasıl bulacaktık? Kurumlar, sahip oldukları verinin bilincinde değillerdi henüz. Belki de şekil, ancak başka yerlerde bulunan noktaların birleştirilmesiyle elde edilecekti. İşte veri madenciliği sorunları gündeme gelirken, geniş veri ambarlarında istatistiksel ve matematiksel teknikler kullanarak çeşitli örüntüler tespit ediliyor. Bu da yapay zekâdan bahsetmiyoruz, sadece istatistik ve matematik kullanılarak birtakım örüntüler, “*patern*” dediğimiz şeyler kullanılıyor.

Peki, bu verilerden ne elde ediliyor? Bir tamamlayıcı bilgi elde edebiliyoruz. Mesela bir yerde AKP'nin oylarının düştüğünü görebiliriz; fakat bu oyların hangi bağlantılar içinde düştüğünü



görmek için veri madenciliği kullanılabilir. Mesela oradakilerin çoğu esnaftır, AKP'nin taksitleri kaldırmasından dolayı esnafın durumu kötüleşmiştir, satışları düşmüştür, bu satışın düşmesiyle beraber de AKP'ye bir tepki oluşmuştur diyebiliriz. Bu verilerden tahmin yapmak için faydalanılabilir. Mesela öğrencilerin sınavlarda aldıkları notlara bakarak üniversite sınavında kaç aldıkları ölçülebilir. Bu veriler öngörü yapmak için kullanılabilir; mesela azami hızın 90 kilometreye çıkması, trafik kazalarının oluşumunu nasıl etkiler?..

Ancak esas önemlisi, sınıflandırma. Veri madenciliği şu amaçlar için kullanılıyor: Dolandırıcılık şüphesi taşıyan kredi kartı işlemleri tespit



ediliyor, bir örüntü oluşturuluyor. Eğer bu örüntüye giriyorsa, o kredi işlemi yapan kişi şüphe altında. Verilecek bir kredinin banka açısından risk taşıyıp taşımadığı, yine veri madenciliğinde bulunabiliyor. Bir sağlık durumu olup olmadığı, bir vasiyetnamenin iddia edilen kişi tarafından yazılıp yazılmadığı, belirli mali hareketlerin terörist tehdit içerip içermediği buradan bulunabiliyor.

Kümeleme yapılabiliyor; belli gruptaki insanlardan belli kümeler oluşturulabiliyor. İlişkilendirme yapılabiliyor ve bu ilişkilendirme uydu görüntülerinin analizinde, elektrik yüklerinin tahmininde, mali tahminlerde vesaire kullanılabilir. 11 Eylül'den sonra ABD'nin yapısı değişti; artık özne temelli analizden örüntü temelli analize geçildi. Birçok profillemeye ve öznel etkene dayalı çalışma yapıyorlar. Mesela bazı terörist eğilimleri hesaplamışlar ve bu hesaplamalara dayanarak kimi zaman Arap, kimi zaman Müslüman, diğer zaman Ortadoğu vatandaşlarını doğrudan gözaltına alabiliyorlar. Bu hesaplamaları yaparken, din ya da doğum yeri bilgisi, terörizm riskini artıran bir parametre olarak işleniyor. Peki veri madenciliği nesnel bir süreç mi? Analiz süreci, veri madenci araştırmacının ideolojisine, önyargılarına dayalı bir şey. ABD'liler bu araştırmayı yaparken, *“Şu şu parametreler bir teröristi tanımlar: Eğer etnik kökeni Arap ise, bunun terörist olma ihtimali yüksektir; Ortadoğulu ise, yine olabilir.”* Tüm bunları matematiksel olarak birleştirerek birtakım analiz yapıyorlar ve bu şeyden sonra uçağa binerken yakalanabiliyorsunuz ya da başka bir yerde doğrudan gözaltına alınabiliyorsunuz.

Şöyle düşünün: Eğer Türkiye'de böyle bir çalışma yapılsaydı -belki de vardır- ne olurdu? Mesela Türkiye'de Arapların ve Güney Amerikalıların yerine kimler geçerdi, hepimiz az çok biliyoruz. Mesela en başında şunu söyleyebiliriz: Türkiye'deki sosyal bilimciler, muhtemelen şöyle derlerdi: *“Gezi'de ölenlerin tamamı Alevi'ydi, Aleviler potansiyel teröristtir...”* Analizlerde Alevilerin daha terörist potansiyeli çıkacağı için, doğrudan onlar gözlem altında tutulacaktı, bu da ortamı daha çok gerecekti.



Büyük veri ya da veri madenciliği dediğimiz şey, eğer insanlık yararına kullanılırsa, çok önemli şeyler elde edilebilir; fakat kontrol edilmediğinde, bu çok ürkütücü olabilir. Mesela bir PRISM skandalında ortaya çıkan şeydi: ABD, Google'dan, Microsoft'tan, Apple'dan, birçok ünlü şirketten tüm verileri alıp kendisi analiz ediyordu, yani PRISM'den çıkan buydu. Büyük veri üzerine analiz yapan tüm şirketlerin ve kamu kurumlarının özerk kamu kurumları tarafından denetlenmesi gerekiyor. Kimi zaman bilgilerin başkalarına verilmemesi konusunda yasalar çıkıyor; fakat Google'ın ya da Facebook'un ne araştırma yapacağını bilemiyoruz. Yaptıkları araştırma sürekli denetlenmesi lazım ki, insanların aleyhine bir şey olmasın, etik kuralları aşan bir şey olmasın.

Gözetim iyi ya da kötü diyemiyorum; çünkü verilerin toplanması, insanlara daha iyi hizmet sunulması için de önemli bir şey, sağlık açısından önemli bir şey. Gözetim, bir mücadele alanı desek daha doğru olacak; insanlığa getirebilecekleri yanında, son derece tehlikeli potansiyel bir güç olarak görmek gerekiyor, yani iktidarların elinde varsa, vay halimize... Zaten Arap baharından sonra ortaya çıktı; oradaki birçok gözetim sistemi doğrudan Avrupalılar tarafından Arap ülkelerine satılmış ve kullanılıyordu. Muhtemelen burada öyle bir olay yaşansaydı, burada da birçok şey çıkacaktı.

Teşekkür ederim.

OTURUM BAŞKANI- Teşekkür ediyoruz.

İzlem, gözetimle ilgili olarak çok enteresan şeylere dikkat çekti aslında; şehir efsanesi gibi olan şeylerin de aslında bir yerlerde kaleme kâğıda döküldüğünü ve bunun üzerinden bazı işlerin yapıldığını ifade etti. Türkiye'yi soracaktım gerçekten, “*Böyle bir şey var mıdır?*” diye. Bizim coğrafyada böyle bir şey söker mi, ondan da çok emin değilim. Gezi'den sonra özellikle ülkede bazı şeylerin değişmiş olabileceğini öngörüydük. Ben son zamanlarda Twitter falan kullanmaktan vazgeçmeye karar verdim. Buraya yönelik de çalışmalar devam ediyor



herhalde. Teşekkür ediyoruz.

Son zamanlarda özellikle Twitter, Youtube yasakları konusunda Ankara Barosunun çok hızlı refleks gösterdiğini biliyoruz. Bu yönde alınan kararlar, aslında birçok tartışma programına da konu olmuş şeyler. Dün Metin Bey bir televizyondaydı, ilk defa devletin bürokratik bir kurumunun olmayan yargı kararlarından bahsetti; bunu yayımladı ve bunu gerekçe göstererek bir şeyleri ifade ettiğini söyledi. Sizler bu konuda çalışmalarınızı zaten yoğun olarak yapıyorsunuz. Söz sizde, buyurun.

Av. YELDA GİZEM ÜNAL (Ankara Barosu Haberleşme Hukuku Kurulu Başkanı)- Teşekkür ederim.

Herkese iyi akşamlar.

Panel gündemine değineceğim, ancak sunum kullanmadan dialog halinde ilerlesin istiyorum.

Bir şeyi merak ediyorum: İçinizde mail, Facebook, Twitter vesaire sosyal medya hesabı olmayan biri var mı? Bir hanımefendi; hiç kullanmıyorsunuz, iyi ediyorsunuz. Peki, kullananlara soruyorum: Sosyal medya hesabınızı -Allah gecinden versin, ama- vefat ettiğinizde ne yaparsınız; normal şartlarda miraslarınız gibi altsoylara devretmeyi mi tercih edersiniz, yoksa İnternet âleminden tamamen silinmeyi mi tercih edersiniz? Bunu birazcık düşünün, bunun üzerine somut örneklerle ilerleyen dakikalarda yine değineceğim.

Panelin konusu bilgi güvenliği. Bilgi güvenliğini TCK anlamında bilişim suçları; adli bilişim, artı bilgi güvenliği başlıklarında değerlendiriyoruz. Bilişim suçları da Bilişim Suçları Daire Başkanlığının kurulması ile

2011 yılından sonra bunların hem hukuki anlamda hem de pratikte gündeme geldiğini varsayarsak, bilgi güvenliğini kapsayan kısmı, en azından veri suçları. Veri suçları da kişilere, kamu kuruluşlarına, devlete ya da mülkiyetinize karşı suçlar olarak üçe ayrılıyor.



İzlem'in konuşmasında, *"Türkiye'de böyle şeyler yapılıyor mu?"* gibi bir şey denildi. Bugün MİT'in sayfasında -telefonu olanlar bakabilirler- bir ilan çıktı, *"Bilgi teknolojileri çalışanı iş ilanı"* gibi bir şey. Tam başlığını hatırlamıyorum, ama şöyle söylüyor: Bir sürü başlık vermiş, veri madenciliği de bunlardan bir tanesi; *"Şu şu başlıklardan herhangi birisiyle ilgili deneyim sahibi"* diyor. Deneyim sahibinden kastının ne olduğu belli değil, somut kriterler aramıyor özellikle. Ben linki görünce şöyle düşündüm: Avrupa'da ve pek çok yerde iyi hackerlar devlet bünyesinde istihdam edilmek isteniyor. Bizdeki de buna benzer bir şey olabilirdi ancak, ilanda : *"Bu bir iş ilanı değildir."* yazılı. İş ilanı değil, ama siz iyi bir hacker'sınız, belli yetenekleriniz var vesaire ve bunu MİT'e üstelik de, yani yapabileceğiniz en büyük kuruluşa alenen beyan ediyorsunuz, *"Ben şu konuda uzmanım"* vesaire... MİT'e bunu açık açık bildirmeye gerek yok, zaten bu tarz bilgilere ulaşabiliyorlar, ama açık bir şekilde bugün böyle bir haberleri vardı. Sosyal medyada bayağı ses getirdi bu, *"Tam olarak ne amaçla yapılıyor?"* diye. Ben de bilmiyorum, bu böyle soru işareti olarak kalsın aklınızda.

Yine bugün Cumhuriyet gazetesinin manşetlerinden bir tanesi şuydu: *"Hemen şifrelerinizi değiştirin."* Okudunuz mu, bilmiyorum. Açık kaynak kodlu bir yazılım mı, tam teknik karşılığını bilmiyorum, ama virüs gezdiğinden ve tüm açık kodlu yazılımlarda mevcut olduğundan, mail adreslerimizin, hesaplarımızın şifrelerinin revize edilmesi gerektiğine dair bir haber vardı. Ben çok yakından iletişim içinde olduğumdan için 2-3 yıldır takip ediyorum, ama eskiden teknoloji sayfalarında haftada bir haberler güncelleniyordu ve sürekli böyle şeyler çıkmıyordu. Şimdi sürekli *"Twitter'a şu oldu, Youtube'a bu oldu"* gibi teknik haberler gündeme geliyor. Dolayısıyla yediden yetmişe herkes için içine girmeye başladı.

Twitter örneğini verdim; Twitter, 5651 sayılı Yasanın değiştirilmesiyle birlikte erişime engellenen siteler arasına girdi ne yazık ki. Çok ses getirdi; çünkü bir sürü kullanıcısı var. Ancak Twitter'a gelmeden önce, zaten 2007 yılından itibaren, yani yasa yürürlüğe girdiği

tarihten itibaren Türkiye’de çok ciddi bir İnternet sitesi erişim engeli söz konusu oldu. Geçtiğimiz hafta Twitter, Baronun ve profesör hocalarımızın Danıştaya yaptığı bir itirazla yeniden erişime açıldı, ama bu sefer de Youtube kapalı kaldı. Youtube sonra bir günlüğüne açıldı. “Gölbaşı Sulh Ceza Mahkemesinin kararı var” diyorlar. Normal şartlarda konuyla ilgili bir sürü karar olabiliyor zaten. Doğal olarak tek bir site am pek çok karar olduğu için, her seferinde ayrı bir tanesini hayata geçirerek siteyi kapatıyorsunuz. Sonra biz siteyi açtırma talebinde bulunuyoruz, 2 gün sonra “Bir de şöyle bir kararı vardı” deyip yeniden siteyi kapatıyorlar.



Aslında bu güvenlik mi; değil. Zaten 5 dakika bile açık olsa, isteyen istediğini yapabiliyor. Kaldı ki siteye erişim hiçbir zaman olmasa bile, bir sürü VPN ve DNS ayarlarıyla vesaire herkesin

erişimi sağlanabiliyor. Teknik olarak yapılan engeller, sansürler, en azından benim nazarımda erişimi engellemiyor. “Sayfa kapandı, ne yapacağız?” falan diyen insan kaldığını sanmıyorum. Iphone’un falan bedava uygulamaları var, indiriyorsunuz, VPN hesabı oluyor, takır takır her şeyi giriyorsunuz. Dolayısıyla kanunen yaptırım olmakla birlikte, bunların pratikte insanların hayatında bir yaptırıma gerekçe oluşturduğunu ben en azından düşünmüyorum.

Yine gündemde olan bir şeyden bahsedeceğim. Biliyorsunuz, yakın zamanda yerel seçimler oldu. Ankara’da değil, ama İstanbul’da şöyle bir şey oldu: Büyükşehir Belediyesinin sanırım, İstanbul’un büyük



meydanlarında ücretsiz İnternet erişimi hizmeti var. İnternete erişimi sağlayabilmemiz için biliyorsunuz, bir şifre uygulaması var, o şifreye erişmek için de önce o sisteme kayıt olmak gerekiyor.

Yani herhangi bir hesaba biz bir oturum açmamız için, orada bir kullanıcı adı ve password oluşturmamız gerekiyor. Dolayısıyla bunu yapmak için de zaten meydanda girmeye çalışıyorsak İnternete, bir telefona, İpad'a vesaireye ihtiyacımız var. Dolayısıyla gayet rahat bir şekilde telefonundan, Wi-Fi'den giriyorum, kullanıcı adı oluşturuyorum, şifre oluşturuyorum, bedava İnternet kullanıyorum. Karşılığında ne oluyor; girdiğim bütün İnternet siteleri, attığım bütün mesajlar, mail'ler vesaire, her türlü trafik bilgisi, içerik bilgisi dâhil, Büyükşehir Belediyesinin kapsamı altında olmuş oluyor. Dolayısıyla diyoruz ya, *"Türkiye'de böyle şeyler yapılıyor mu?"* Türkiye'de böyle şeyler çok aleni yapılıyor aslında, ama *"Meydanlarda bedava İnternet var, ne güzel"* şeklinde bundan karşılıklı fayda sağlanıyor. Hâlbuki bu, bizim İnternet faturamıza belki olumlu yansıyor, ama aynı zamanda daha büyük pencereden baktığımızda, hem devletin "fişlemelerine" hem de saha araştırmalarına, veri havuzlarına ne yazık ki biz kendi elimizle katkı sağlamış bulunuyoruz.

Az önce sorduğum soruya geleyim; cevap verebilecek olan var mı? İnternet hesaplarınızı, sosyal medya hesaplarınızı ne yaparsınız; miras mı bırakırsınız, şifrelerinizi birine mi bırakırsınız, yoksa İnternette sizinle ilgili olan her şeyin silinmesini mi tercih edersiniz? Var mı buna cevap verecek?

SALONDAN- Silinmesini tercih ederim.

Av. YELDA GİZEM ÜNAL- Neden silinmesini tercih edersiniz?

SALONDAN- Zaten sonuna gelmişim.

Av. YELDA GİZEM ÜNAL- Peki, siz varken var olmasını tercih eder misiniz?



SALONDAN- Benim kontrolüm altında...

Av. YELDA GİZEM ÜNAL- Ama internette sizin kontrolünüz altında olmuyor ne yazık ki.

Şöyle bir somut olay var: Ben Ankara Barosu mensubuyum. Baronun Baro levhası var; orada cep telefonları, adresler, kimlikler vesaire bir sürü bilgimiz var. Bu sadece Baroyla ilgili değil, birçok kurum ve kuruluşla ilgili- telefon numaralarımızı, adreslerimizi vesaire özel şirketlere satıp bundan ufak da olsa bir menfaat elde ediliyor ya da reklam yasağı dâhilinde bir getiri sağlıyorlar bildiğim kadarıyla. Buna bile gerek yok, siteye girip ulaşabiliyorsunuz da zaten. Ben kendimi arıyorum İnternette ve hiç alakamın olmadığı Avukat İletişim, Avukat Portal, avukat bilmem ne, bir sürü İnternet sitesinde ismim, adresim, telefonum, mail'im, her şeyim yazıyor. Birçok avukat sürekli ofis falan değiştirir; mesleğe ilk girdiğimizde, birinin yanında sözleşmeli çalışırız, sigortalı çalışırız vesaire... Baro levhasında adres yenileyebiliyoruz, ama her İnternet sitesinde bunları yayımlayamıyoruz ne yazık ki.

Türkiye'de bunun yasal dayanağı yok. 2010 yılında bu anayasa değişikliğiyle 20. maddedeki özel hayat kuralı birazcık genişledi, özel hayatın gizliliği bir hak haline geldi. Ancak anayasada hak haline gelmiş olması, diğer uygulamadaki yasalarda ne bir karşılık bulmadığı için, pratikte de bir sonuca ermedi. Dolayısıyla İnternette -esasından Avrupa'da ve Amerika'da da bunun bir sürü hukuki karşılığı artık oluştu- unutulma/silinme hakkımız var; bir başvuruyla bütün adımlara yazılı siteler vesaire, yani bizim kabul ettiğimiz ya da etmediğimiz harici şeyler engellenebiliyor. Ancak bunun Türkiye'de hukuki bir karşılığı yok.

Türkiye'de şöyle oldu: Bir avukat arkadaşımın önemli bir tebligatı ofisine ısrarla gelmedi. Bunun için mahkemesine yazı yazdı, Baroya yazı yazdı vesaire... Sürekli karşı taraf vekili, adresi İnternette bulduğu için, İnternette de bir sürü ofis değişikliği yaptığı için, bir



türlü bunlar anlayamadılar. Kaldı ki bunun MERNİS gibi bir çözümü var, MERNİS'te de aksaklıklar oldu vesaire... Tazminat davasına gitti konu, avukatın adresine gelmemesinden kaynaklı uğradığı maddi-manevi zarar ! Enteresan, oradan sonuç çıktı, MERNİS adresinde de tabii ki aksaklık olduğu için. Muhtemelen MERNİS'te sorun olmasaydı, bir sonuç çıkmayacaktı, ama oradan bir karara bağlandı. Dolayısıyla Türkiye'de unutulma hakkı, hak olarak yasalaşmamış olsa da pratikte alternatif çözümlerle yapılabilir bir şey haline geldi.

Bunun Amerika'da bir örneği var; zaten ilk unutulma hakkı da bu somut olaydan çıkıyor. Avustralyalı birisi galiba, Amerika'da bir suçla karışıyor. Sonra İnternette her aramada Amerika'nın işte büyük uyuşturucu baronlarıyla falan haberleri çıkmaya başlıyor. Adamın işi, eşiyile ilgili sorunlar oluyor ve adamın kariyerinde ciddi bir çizik oluyor. Sonrasında adam, İnternetteki adına yapılı tüm haberlerin yayından kaldırılmasını talep ediyor. Tabii her siteye ayrı ayrı içeriğin yayından kaldırılmasını talep edemezsiniz; kaldı ki yurtdışında ya da bizim erişemediğimiz, onların erişebildiği vesaire İnternet siteleri var. Sonuç olarak, bu taleple yasaların da değişmesiyle birlikte yurtdışında olabilen bir durum, bizde de olmasını umuyorum.

Buraya neden geldim; kişisel veri güvenliğimizden geldim. Kişisel verilerimiz çok basit yollarla herkesin eline geçiyor. Mesela Adınızı, soyadınızı yazıyorsunuz, hatta yazmasanız da oluyor; mesela Yelda Gizem'i yazın, diğer harfler bile otomatik çıkıyor. Tıkılıyorsunuz, TC kimlik, adres, ne varsa İnternette, bütün bilgiler dökülüyor; anne adı, baba adı, cilt no, sıra no falan... Onları alıp başka bir İnternet sitesine yüklediğinizde, oradan diğer hesaplara ulaşıyorsunuz. Aslında devlet eliyle bilgilerimiz gayet rahat bir şekilde İnternette geziyor, buna sağlık bilgileri de dâhil. Bu çok sansasyonel haber oldu yakın zamanda, belki takip etmişsinizdir; eczanelerdeki ilaç alma durumları... Aslında bu bir yandan işi kolaylaştırıyor, yani buradan Diyarbakır'a da gitsen, TC kimlik numarasıyla hangi hastalığı geçirmişiz, hangi ilacı kullanmışız, hangi ilacı nereden ne şekilde almışız, hepsi mevcut.

Tabii bunlar bir şekilde her ne kadar hayatı kolaylaştırıyor olsa da esasında 3 kişilerin kişisel verilerimize erişmesinin önünü açıyor.

Mesela İnternete giriyoruz, “18 yaşından büyük müsünüz? Kadın mısınız, erkek misiniz?” bir sürü buton oluyor. Yapmak istediğimiz şeye ulaşmak için sürekli “evet” diye hiç okumadığımız fersah fersah sözleşmelere imza atıyoruz. Dolayısıyla sonra mağdur oluyoruz, dilerim somut olarak karşılaşmamışsınızdır.

Yine bir örnek vereyim: İnternet sitelerinde; seçimlerle ilgili, onun öncesinde devletle ilgili pek çok olayda “Değiştir, imza at; değiştir, tek imzayla şöyle olsun, böyle olsun” gibi kampanyalar düzenliyorlar.



Ben, az önce İzlem Beyin bahsettiği gibi, sosyal medyayı fazla aleni kullanan birisiyim, gizliliğe, güvenliğe falan çok önem vermiyorum; çünkü zaten önem versek de isteyen, istediği şeye ulaşabiliyor.

O nedenle bu tarz sitelerde aslında imza atıyorum, Ancak şöyle şeyler oluyor, mesela diyor ki, “40 bin tane imza atılacak, 40 bin imzanın karşılığında şöyle şöyle bir şey yapılacak.” 40 bin imza olması için herkes birbirine link yolluyor vesaire... Birisi, esasen başka bir sisteme müdahale ederken, o sırada gelen mail’e tıklıyor, imza kampanyasını da hack’lemiş oluyor, o sırada yapmaya çalıştığı şeye o da dâhil oluyor. Elinde 40 bin skala olduğu için, 40 bine yakın kişinin adı, soyadı, TC kimliği vesaire oluyor. Sonra bunu araştırıyorlar ki, çoğu hukukçuların ya da bürokratların vesaire, yani resmi kanalların, devlet



çalışanlarının bilgileri. Bu somut olay çok komplike bir durum, bir sürü şey için.

Sosyal medyada korunmak için, bilgi güvenliğimiz için, güvenilir bilgiye ulaşmak için ne yapılabilir? Alternatif Bilişim Derneği'nin bir projesi var, “*Kem Gözlere Şiş.*” İnternet sitesini ziyaret ederseniz eğer -reklama girmiyordur umarım, bence girmiyor- “*Kem Gözlere Şiş*” şu: Gerek telefondan, taşınabilir aygıtlardan gerek masaüstü bilgisayarlardan gönderdiğiniz mail’leri şifreliyorsunuz ve İnternette anonimleşmeyi sağlayan yöntemler ediniyorsunuz.. Çünkü attığımız adım iz bırakıyor. Mesela Google’da bir şey arıyoruz, sonra sürekli onun reklamı gelmeye başlıyor her yerden, sürekli yandan “*banner*”ler çıkıyor falan... Bir şekilde hem resmi kanallardan hem resmi olmayan kanallardan takip ediliyoruz.

Dolayısıyla bilgi güvenliği anlamında herkesin kendini koruması gerekiyor. Zaten esasen bu korumada her ne kadar sistemler çok güvenilir, ağlar çok kontrollü gibi görünüyor olsa da esasında koruma insandan kaynaklanıyor. Bu nedenle, umarım daha güvenli İnternet kullanabildiğimiz günler olur. Gerçi 5651 sayılı bu İnternette yapılan yayınlarla ilgili olan yasa değişti ve arkasından da birçok insan daha fazla mağdur oldu. İçinizde şahit olan var mı bilmiyorum, ama Twitter.com, Twitter.com/yeldagizem mesela, ben bir şey paylaşıyorum. Normal şartlarda hukuka aykırıysa eğer ve ondan birisi mağdur oluyorsa, zaten bunun bilişim suçları dâhilinde olmasa da bir karşılığı var; birine hakaret ediyorsanız, tehdit ediyorsanız vesaire... Yani sadece yüz yüze yapmıyorum da İnternet üzerinden yapıyorum bunu. Ancak son zamanlarda biraz da popüler kültürle alakalı olmakla birlikte, sosyolojik de bir durum var. Ankara’da, İstanbul’da vesaire herkes çok İnterneti kullanıyor, İstanbul’da Wireless yapmak çok ses getiren bir şey oluyor, ama buradan biraz doğuya doğru gidiyoruz, meydana İnternet olsun-olmasın, herkesin cebinde akıllı telefonu olmuyor. Dolayısıyla İnternette bilgi güvenliği önemli olmakla birlikte, bunun -hukukçu olarak söylüyorum, ama- şahsen çok önemli olduğunu



düşünmüyorum; çünkü her halükârda ulaşılmak istenilen şeye zaten çok rahat bir şekilde ulaşıyor. Ancak bu bilgi güvenliği durumunu sağlamak için trafik kayıtlarınıza dikkat etmenizi öneriyorum.

Teşekkür ederim.

OTURUM BAŞKANI- Biz de teşekkür ediyoruz.

Aslında bu tarz konulu panellerde şöyle bir tehlike var: Panel sonunda giderken, bir yandan buradan bir teknoloji düşmanı olarak çıkabiliyorsunuz; çünkü o kadar enteresan şeyler oluyor ki, “*Teknoloji kullanmayalım, lanet olsun*” diyesi geliyor insanın. Ancak hayatımızın artık bir parçası olmuş ve Gezi sürecinde mühendis camiası olarak mesleğinden bu denli utanan kesimlerden birisiyiz. Baroya bakıyoruz, avukatlar koşturuyor, gözaltına alınanlar için mücadele ediyor, yayınlar yapıyor, doktorlar sağda solda müdahale ediyorlar. Biz mühendisler ne yapıyoruz; bizatihi o olayların çıkmasına sebep olan projeleri biz üretiyoruz; oradaki o kadar gaz bombasını, gaz fişliğini, o araçları vesaireleri falan... Bazen o noktaya geliyoruz gerçekten.

Siz Wi-Fi’lerin İstanbul meydanlarında olmasından bahsettiniz. Bizim burada da başka bir durumumuz var; Melih Gökçek kendisini korumaya alıyor ve Belediyeye 150 bin liralık bir güvenlik duvarı alıyor sanıyorum, bu manşetlere taşınmıştı. Buradan da size paslayalım, siz ne diyeceksiniz bakalım.

Buyurun.

ENGÜR PİŞİRİCİ (Bağımsız Siber Güvenlik Araştırmacısı)- Ben öncelikle bu güzel ortam için teşekkür etmek isterim.

Ben burada biraz daha kafalarınızı karıştırmak, ama bazı konularda aydınlatmak adına biraz şeytanın avukatlığını oynamak isterim.

İnternet olgusunu çok yanlış anlıyoruz genellikle, gerek hukukçuların gerek mühendislerin gerek sosyologların gerek insanların kafası



karışık. Bunun en büyük sebebi, bir devrimi yaşıyoruz ve içindeyiz. Bu devrime de bilgi devrimi diyebilirsiniz, kaynaşma devrimi diyebilirsiniz. Kısaca İnternet bir devrim ve hayatımızın ayrılmaz bir parçası, İnternet yaşamdır diyebiliriz.

Ben arkadaşımızın size sorduğu soruyu biraz daha genişleterek tekrar sormak istiyorum: Sosyal mecrada kullandığınız hesapların kendinize ait olduğunu düşünüyor musunuz? İnternette erişim için kullandığınız kaynakların bir satılma olgusu, bir satılma aracı olduğunu düşünüyor musunuz, satılabildiğini düşünüyor musunuz? Yani bir alan adı satın aldığınızı mı düşünüyorsunuz, yoksa o alan adı aslında size ait değil mi? Bunlar aslında bir toplu kabulleniş. Alan adını siz 10 seneden fazla kullanımınıza tahsis edemezsiniz, bunların hepsi bir kabullenıştır, IP bir kabullenıştır. Siz bilgisayarınızın ayarlarında DNS ayarı girerken, bir kabullenişle siz o DNS'leri kullanacağınızı söylüyorsunuz. Twitter.com adresine o IP numarası girdiğiniz DNS sunucusu size söylüyor. Başka bir sunucu yazarsanız, o başka bir yer de söyleyebilir. Bunların hepsi bir toplu kabullenıştır. Örnek olarak Twitter.com, bir gün şirketi kapatıp gittiği takdirde, siz hesabınızı alıp bir başka yere taşıyabileceğinizi mi zannediyorsunuz? Facebook kapandığı takdirde, Facebook'taki hesabınızı alıp “myspace” ya da “org” diye bir başka sosyal mecra sitesine götürebileceğinizi mi zannediyorsunuz; değil.

İnternet olgusunu doğru anlamak çok önemli. İnternette sahip olunan tek şey, sizin ürettiğiniz içeriktir; bu bir yazınız olabilir, paylaştığınız bir video olabilir, koyduğunuz bir müzik olabilir. Ancak İnternet erişim kaynakları -kaynaklar derken alan adları, IP numaraları, bunun gibi şeyler- toplu kabullenişle dünyaya aittir, kimsenin bir malı değildir. İnterneti demir yumrukla yöneten Amerika, İnternet yapılanmasını biraz incelediyse, bir kurum var, ICANN diye. 2003 yılında ICANN'de bir tartışma oldu. DNS'i Amerika yönetiyordu. Dediler ki, “*Bu toplu kabulleniş, sen tek başına yönetiyorsun. Biz bunu değiştirelim*” ve alternatif DNS kavramları çıkmaya başladı. Amocanc, bunu bütün İnternet toplumuna, dünyaya açtı ve her milletten insanlar



bunlara katılmaya başladı. En son ICANN'den de daha yukarıda olan, bu “resources”ların dağıtımından sorumlu olan IANA'nın da artık Amerika'nın kontrolünden çıkıp -bu sene içinde onu göreceğiz- dünyanın kontrolüne girdiğini göreceğiz ve İnternet gerçekten özgürleşmiş olacak.

DNS konusunda bir ufak ekleme yapmak istiyorum: ICANN, geçtiğimiz sene bir program başlattı. DNS'te bir cast'ımız vardı, TLD dediğimiz “top level domein”, en yüksek alanıdır. DNS, bildiğiniz gibi, sağdan başlayarak noktalar halinde sola doğru çözümlenir; .com, .org, .net gibi alt alan adlarımız vardır. Bunlardan yaklaşık 30 küsur tanesi şu an hayattayken, ICANN, yerel dillerde olmak üzere toplam 1 930 küsur tanesini kabullenmiş ve onları yavaş yavaş hayata geçirmeye başlamıştır. Maalesef ki Türkiye'de pek vizyon sahibi bir oluşum yok, bir tüzelkişilik yok. İstanbul Büyükşehir Belediyesi sadece buna başvurmuş ve “.ist” ve “.istanbul” diye iki tane “top level domein”i kendisi için almıştır, yakında da hizmete girecektir zannediyorum.

Burada insanların korkularından bahsederken, özellikle Türkiye'de yaşadığımız durumlar gerçekten çok tehlikeli sınırların üstüne de geçti. Bazı yanlışlıklar da yapmaya başladık. Biraz korkutacak, ama bu yasakları delmek için kullandığınız VPN olsun, TOR olsun -TOR'u duyan var mı, TOR da bir nevi VPN gibi çalışıyor trafiğinizi “anonimleştirmeyi” sağlıyor, çünkü bunlarda da kötü niyet çok rahatlıkla ortaya çıkabiliyor- bir İnternet sunucusuna bağlandığınız takdirde, siz bütün trafiğinizi bir firmanın eline emanet ediyorsunuz. TOR'da da bilmediğiniz insana emanet ediyorsunuz. Bunlarda kötü niyet, çok rahatlıkla uygulanabilir sistemler olabiliyor.

Bu arada arkadaşımızın bahsettiği bu hatadan bahsetmek istiyorum, bu aslında çok önemli bir şey. Gazeteler maalesef yanlış yazıyor, bir virüs diye bahsediyorlar. “Open SSN” kütüphanesinde bir hata çıktı. “Open SSN” ne demek, onu anlatayım kısaca: Web tarayıcılığınızda güvenli olarak İnternet kullandığınızı düşündüğünüz an, aslında



güvende olmakla güvende hissetmek ayrı şeyler. Bir bilim adamı demiş ki, *“Bu İnternetteki güvenlik kavramı bir tiyatrodur; size sahnelerler, siz güvende olduğunuzu hissedersiniz, ama aslında gerçekten güvende misiniz, bilemezsiniz.”*

Mesela bir bankaya girdiğiniz takdirde, neye dikkat edersiniz; URL’yi yazdığınız adres çubuğunda bir yeşil bağlantı, bir anahtar simgesine bakarsınız, o sizin güvende olduğunuzu hissettirir size. Anlatırlar, *“Biz 128 bit’lik bir anahtar şifrelemesi kullanıyoruz, bir elektronik sertifika denilen bir şey aldık, siz bununla güvenle bizim bankaya bağlanabilirsiniz”*

derler. Bu sadece bankalar için mi geçerli; hayır, kullandığınız e-posta hizmet sağlayıcısından tutun da mühendisler için şu an zorunlu bir şey yok, ancak avukatlar için



elektronik imza var mesela, UYAP için onların kullanımına kadar... Keza Hercsemben Şirketinin 1 Ocak 2014’ten itibaren *“kaiten tuto”* posta alması zorunluluğu oldu. Hepimiz çalışanız burada, muhakkak tüzelkişiliğimizde de *“kaiten tuto”* postayı göreceğiz, ki elektronik tebligat adresi olarak geçer artık kanunda. Orada kullandığımız, oyun için girdiğimiz, muhabbet için girdiğimiz, kendimizi güvende hissettiğimiz, yani İnternetin güvenli temelini oluşturan sistemde -ki İnternette bu yaklaşık yüzde 70’i kapsıyor- bir bulanana açık.

İnternetin yüzde 70’ini kapsayan bu açık şunu yapıyor kısaca: 2011’de aslında yazılım kütüphanesine girmiş, 2012’den beri piyasada bulunan, 2014’te sadece *“disclose”* olan, yani halkın duyduğu -ki



bundan önce başkaları çok rahatlıkla duymuş olabilir, biraz sonra ona da değineceğim- bir açıktan bahsediyorum. Basitçe sizin bu Web tarayıcınızla bağlandığınız sunucunun hafızasını “dump” ediyor. Bu ne demek; o hafızada ne var? Çok paralarla satın alınan o Web sitesinin elektronik sertifikası var, onun gizli anahtarı var. O Web sunucusunu kullanan, eğer bir e-posta hizmet sağlayıcısıysa bu, e-posta parolaları ve kullanıcı isimleri var, e-postalar var. Bir sosyal mecra sitesiyse, insanların yazışmaları var. Kısacası o sunucunun hafızasındaki her bir şeyi sunucuya bir “log” düşürmeden karşı tarafa iletiyor. Bu, şu demek: Sizin şu ana kadar İnternette gezindiğiniz yaklaşık 3 siteden 2’si bu halde, 2 senedir bunu böyle yapıyorlar. Muhtemelen sizin bütün kullanıcı adı ve parolalarınız şu an başkalarının elinde olabilir.

Snowden’i duymuşunuzdur; Wikileaks’teki “manning”’den sonra bir CIA analisti kaçtı ve Snowden, dokümanlarını yayınlamaya başladı. NSA’nın birkaç senedir bütün dünyayı, ki arkadaşımız çok güzel söyledi; eskiden telefon dinlemeleri olsun, bir gözetim olsun, bir personelin bunu yaptığını düşünüyorsunuz, ama şimdilerde bilgisayarlar bunu yapıyor ve milyonları takip ediyorlar. Obama da bunu kabullenmişti, NSA’nın uyguladığı bir gözlem sistemi tüm ülkenin trafiğini izliyor ve “*Bunu bir ülkeye deploy ettik*” diye ortaya çıktı. O ülkenin ismi çıkmadı 2009’dan beri, bu büyük ihtimalle Türkiye olabilir. Komplo teorisi, bunu ispatlayamayabiliriz, ama yaşananlar, özellikle 2009’dan sonra çıkan görüntüler bunu gösteriyor. Bütün ülkenin e-posta trafiği, faks trafiği, telefon trafiğini gözetlemeye yarayacak bir sistem ve bunu bir ülkede deplow ettiklerini kabullendiler, NSA’ın bu sızan dokümanlarında vardı.

NSA’ın bu şifreli trafiği nasıl izlediği tartışılıyordu; özellikle kriptocular, kripto analistleri, matematikçiler tartışılıyordu, “*Kardeşim, bunlar bir özel matematik mi keşfettiler de bu bilgisayarların kıramayacağı şifrelerin algoritmalarını bir şekilde kuruyorlar?*” Dokümanlar yayımlandıktan sonra şunun farkına vardılar: Dokümanlardaki ifadelerde NSA’ın bunları kırdığı değil de çözdüğü



olarak geliyordu. Kelimeler çok önemlidir; kelimeleri doğru yerde kullanmazsanız, farklı anlamlar elde edersiniz. Örnek olarak şifre mi, parola mı; kullanıcı adı yanında siz şifre mi girersiniz, parola mı girersiniz?

SALONDAN- Parola.

ENGÜR PİŞİRİCİ- Şifre nedir peki?

SALONDAN- Algoritma...

ENGÜR PİŞİRİCİ- Aynı değil. Etnolojiye bakarsanız, şifre bize Fransızca'dan gelmiş, "*chiffre*"dan gelmiş. "*Chiffre*" da onlara Anglosakson olsun, Frank olsun, Germenler olsun, Ortaçağ Avrupa'sında Arapça'dan gelir. Araplar cebiri keşfettikten sonra, Ortaçağ'daki Avrupa bunu almaya başlarken, ki o zamanlar Roma rakamlarını biliyorlar, hesaplamayı ona göre yapıyorlar ve Araplar kalkıyor, sıfır diye bir şeyden bahsediyor, cebirin temeli. Sıfır deyince adamlar anlamıyor, sıfır bildiğiniz gibi bize Arapçadan gelmiştir. Onlar da sıfırını "*chiffre*" olarak bir giz, bir gizem, anlaşılmayan bir şey olarak dillerine sokuyorlar. Bize Fransızca'dan Arapça sıfır, şifre olarak geliyor, Arapça'dan bize direkt olarak sıfır olarak geri geliyor. Yani aynı kelime iki farklı anlamda bize geliyor. Ama "*login password*" karşılığı, "*password*"ün karşılığı paroladır. "*Chiffre*" günümüzde kriptoloji alanında kullanılır, şifrelemekten gelir. Kullandığımız şey şifre değil, paroladır. Neyse...

"Çözüyor" kelimesi çok önemli, çünkü NSA'nın bunun nasıl çözdüğünü bilmiyorlardı; bir matematik denklemi keşfettiklerini zannediyorlardı, bu da kompo teorisi. Ama bu "*bug*"la beraber -ki bu yaklaşık 48 saat önce "*disclose*" oldu, dünyaya haberi düştü- şimdi anlamaya başladılar; çok rahatlıkla kurulan bir sistem, herhangi bir Web sitesinin kendisine yönlendirilmesini sağlayabilir. Bu açık anahtarlı altyapı dediğimiz sistemde tamamen aykırı, ama anahtarını biliyorsanız, dinlemeniz mümkün.



Türkiye’deki duruma bakarsak, Türkiye bunun ucuzuna kaçmış durumda. Elektronik Haberleşme Kanunu olsun, güvenli haberleşmeyle ilgili yönetmelikler olsun, anlamlandıramadığı her veri için size cezayı koşar, “*Gelin benden izin alın*” der, ama aynı zamanda kapalı kapılar arkasında şunu yapar: Mesela geçtiğimiz sene Türkiye’de elektronik sertifika sağlayıcı birkaç tane firma var, bunlardan bir tanesi Türktrust. Türktrust’ın bir kök sertifikası, bu ne demek; “*Dünyadaki bütün siteler için ben sertifika üretebilirim*” demek. Peki, bu ne demek; “*Sizin kullandığınız tarayıcılar, beni güvenli buluyor*” demek ve benim ürettiğim bir sertifika, ben mesela www.twitter.com benim desem ve buna sertifika versem, sizin tarayıcınız onu yeşil olarak gösterecek ve Twitter’a girdiğinizi zannederken, aslında benim kurduğum düzeneğe girmiş olacaksınız. Orada artık ne yapıyorsanız, “*mysql log*’unu tutabilirim demektir.

Geçtiğimiz sene Türktrust’ın bir kök sertifikası, İ. Melih Gökçek’in yönetiminde olduğu EGO’dan çıktı ve nasıl çıktı? Aralık 2013’te Google bir uyarı yayınladı. Google’ın kullandığı *Chrome*, bu tip aldatmalar için sertifikaya güvenmekle kalmayıp kendi sertifikası mı, değil mi diye Google için özellikle bakarken uyarı verdi. Meğerse EGO’daki kullanıcılar, bilmeden maalesef başka sitelere gitmeye çalışırken, aslında bütün trafiklerini EGO’nun önündeki cihaz log’luyor. Bu ortaya çıkan bir şey. Bunun bir benzeri *Diginotar*, Hollanda’nın en büyük sertifika sağlayıcısı yaşamıştı ve iflas etti. Türktrust’a ne oldu; hiçbir şey.

Bu yasaklamaları görüyoruz; aceleden, panikle, artık koydukları kanunları bile hiçe sayarak maalesef ki bizim meslektaşlarımız çok acı kararlar aldı. Twitter’ı engellemek için neler yaptılar; sırasıyla sayalım: Önce DNS’den engelleme yapıp kendi DNS’lerinde www.twitter.com’u başka bir yer gösterdiler. Orada bir site çıkıyor ve sitede bir mahkeme kararı yazısı çıkıyor. İnsanlar nasıl geçmeye başladı bunu; DNS değiştirdiler. Daha VPN’e gerek yok; çünkü IP bazlı sınırlama yapmıyor. Sonra ne yaptılar; IP’lerini yasaklamaya çalıştılar.



Onu beceremediler; çünkü Twitter.com büyük bir firma ve bir sürü IP kullanıyor. 4 IP'yi yasakladılar, ama millet diğer IP'lerden bağlanmaya devam etti. Ama daha sonra ne yaptılar; kendi koydukları kanunları bile hiçe sayarak, Google DNS'lerini kendileri bloklamadılar, kendileri cevap verir hale getirdiler. Bu ne demek; siz 888'e, yani Google'ın o ünlü DNS'ine gittiğinizi zannederken, siz aslında Telekom'un Ulus'taki merkezindeki bir bilgisayara gidiyor oluyorsunuz ve oradaki makine cevaplıyor, ama bunu siz bilmiyorsunuz, o Google gibi size cevap veriyor. Klasik anlamda “*pin cherck in*” diye bir komut vardır, cevap veriyor mu, vermiyor mu, ona bakarsınız, size 7 milisaniye cevap döner, yani Amerika'da olması gereken bir sunucu aslında burnunuzun dibindedir. Işık hızıyla gidip gelse, 4 milisaniye yaklaşık birkaç bin kilometre eder, o da Türkiye sınırından çıkmaz.

Peki, bu ne demek; Türk Telekom'u ve *Superonline*'ın ve diğer 277 tane İnternet servis sağlayıcının kendi bacaklarına kurşun sıkması, artı bizim hukuk sistemimizin kendi bacağına kurşun sıkmasıyla aynı anlama geliyor. Çünkü bir adli vakada size kolluk kuvveti, “*Şu IP'den girilmiştir*” cevabını bu İnternet servis sağlayıcıları dönecektir.

Artık bunu görüyoruz ki, en büyük bu servis sağlayıcılar bile, bu IP'leri kendi istedikleri gibi kendi makinelerine yönlendirebiliyorlarsa ve bunu hiçbir hukuk kisvesi altında yapmıyorlarsa, o zaman bu adli vakalarda da niye size düzgün log'ları, düzgün cevapları dönsünler? Yani kısaca hukuk sistemimiz de aslında bir garabeti





yaşıyor, çok korkutucu oluyor. Kısaca VPN'e de girmeyin, TOR'a da girmeyin, onu da söyleyeyim.

Bu sosyal mecralardan sonra, dünyadaki duruma da bir bakarsak, aslında biraz gizli gizli yapıyorlar. Mesela NSA'nın yakalanmasından sonra bir açıklaması oldu, *“Merkel'i dinledik”* diye ortaya çıktı. Özur dilediler mi? *“Bir daha dinlemeyeceğiz”* dediler mi? Ne dediler? *“Bir daha yakalanmayacağız, yakalanmamak için elimizden geleni yapacağız”* dediler.

Bilgi güvenliği ve güvenilir bilgi deyince, aslında yine kelime ve kavram karmaşasına sürükleniyoruz. Aslında çok güzel bir isim, biraz sonra niye güzel olduğunu göreceğiz. Bilgi güvenliği, aslında bilgi güvenliği mi, bilişim güvenliği mi, siber güvenlik mi, ne düşünüyorsunuz? Bu bence biraz üretmememizden kaynaklanıyor olabilir. Dünya çözmüş, DIKW diye bir şeyden bahsediyorlar, *“Data Information Knowledge Wisdom.”* Diyolar ki, *“Data”, “information”*ın alt kümesi, *“information” “knowledge”*ın alt kümesi, *“knowledge da wisdom”* alt kümesi. Mesela bir yağmur örneğiyle açıklarsak; yerde su var, hava 2 derece, bu bir data oluyor. Bunları birleştiginiz vakit, biraz yorum da katarak bir *“information”* üretiyorsunuz, *“Yağmur yağmış”* diyorsunuz. *“Knowledge”*a ekliyorsunuz, *“Dünyanın bu bölgesinde, bu mevsimde yağmur yağar”* diyorsunuz. *“Wisdom”*ı ekliyorsunuz, *“Yağmur yağıyor ve biz hayattayız”* diyebiliyorsunuz.

Peki, bizdeki information karşılığı ne burada; bilgi mi, öz bilgi mi, malumat mı? Datayı veri diye isimlendiriyoruz, *“knowledge”*ı ne diye isimlendiriyoruz peki? *“Knowledge”*a ne dememiz gerekiyor? Know bilmek, *“knowledge”* bilgi. Peki, o zaman *“information”*, malumat... Yani bazı şeyleri dilimize çevirirken anlam kaymaları da yapıyoruz. Bu bir şey üretmediğimizden kaynaklanıyor diye düşünüyorum. Mesela örnek olarak bu *“Data Information Knowledge Wisdom”*ın dışında, bu ülke yıllarca özgür yazılımı serbest yazılım olarak tercüme etti. Daha sonra bir katil balinanın bir filmi çıkmıştı ortaya. Oradaki *“free”* diye



kastedilen, biz o “free”yi başka anlamıştık dedik ve özgür yazılım olarak, “özgür” kelimesi vurgusunu o zaman orada gördük.

Güvenlik alanında saldırı tespit cihazları denilen, aslında “intrusion detection”dan gelen, aslında saldırı olmayan, ama maalesef dilimizde kullandığımız ya da yine şu an bu Siber Güvenlik Eylem Planı çerçevesince Türkiye’de Türk Standartları Enstitüsüne görev verildi, sızma testi, o da “penetration” testi diye geçiyor. Ki “penetration” sızma mı, o da tartışılır bir şey. Basitçe aslında biz dil konusunu pek beceremiyoruz, ben onu görüyorum.

Bilgi güvenliğinden kastımız, bazen bilişim güvenliği oluyor, bazen malumat güvenliği oluyor, bazen harbiden 3 bin senelik bir bilgi güvenliği kavramından da bahsediyor olabiliyoruz.

Peki, bilgi güvenliği ne demek, güvenilir bilgi ne demek? Bilginin güvenliğinden anladığımız şu olabilir mi? Bizim kontrolümüz içinde kalan, bizim istediğimiz kişiye, istediğimiz zamanda, istediğimiz formatta, istediğimiz kadarıyla verilen. Güvenilir bilgi ise, bilgiye eriştiğiniz yerin kaynağının kim olduğundan emin olduğunuz ve bu emin olmanın yollarından da emin olduğunuz bir kavram. Yani aslında iki uç, bence güzel bir isimlendirme olmuş.

Peki, bu açıdan bakarsak, şu an Türkiye’nin ve dünyanın durumu ne? Çok büyük bir dezenformasyon var. Dezenformasyonun kelime anlamına bakarsak, o kadar çok bir bilgi kirliliği yapıyorlar ki... Peki, bunu niye yapıyorlar? Bilgi güvenliğinin bir konsepti, eğer İngilizceden devam edersek, “information security”, bunu bilişim güvenliği de diyebilirsiniz, başka isim de koyabilirsiniz. “Information woldfire” denilen bir kavramımız var. Daha önce elektronik “woldfire” elektronik harp konusunda alt dal olarak çıkmış, ama daha sonra tek başına bir dal olmuş, Amerikan Silahlı Kuvvetlerinin doktrininde yer alan bir kavram, bilişim harbi, bilgi harbi. Orada 3 önemli kısım var, dünyada şu an onu görüyoruz artık; “Information operations”, “computer network attack”, “computer network defence.”



“Information operations”ta ne var; dezenformasyon var, manipülasyon var.

NATO, yanlış hatırlamıyorsam, 2011’de siber uzayı da savaş alanı olarak kabul etmekle beraber, karşılığının aynı yerde olmayabileceğini de söyleyerek bir doktrini kabul etti. Bu ne demek? “Siz siber uzayda saldırırsanız, ben sizin kafanıza füzeyi atabilirim” demek. Peki, siber uzaydaki bu saldırılar, günümüzde çok fütüristik mi kalıyor? “Stux.net”, duyanınız var mı? Muhtemelen bu Amerika Birleşik Devletlerinde ‘olimpic.games’ kod adlı, İsrail, ABD ve Almanya işbirliğiyle hazırlanmış bir dizi siber silah. Ne yaptılar? İran’daki bir nükleer santral için olası bir nükleer yakıt, onların dediğine göre, zenginleştirme tesislerindeki santrifüjlerde bulunan... Kısaca anlatmak gerekirse, uranyumu zenginleştirmek ne demek; içindeki belli bir izotopun yüzdeliğini artırılıyorsunuz. Bunun için ne yapıyorsunuz? İzotoplar kimyasal olarak aynı özellikleri gösterir, o yüzden ayırmaları zordur. Florla birleştirip uranyum florür gazı çıkartıyorlar. İzotoplar sonuçta molekül olarak birbirinden farklı ağırlıkta, döndürüyorlar basitçe gazı. Git gide daha ağır moleküller daha dışarıda, daha hafifleri daha içeride olmak üzere ve bunların da yüzlerce bu alette olduğunu düşünün, santrifüjlerin olduğunu düşünün, böyle kocaman bir araziye serilmiş bir tesis düşünün, orada “scada” sistemleri var Siemens’in ve basitçe yaptığı şey şu oluyor: O “scada” sisteminiz, spesifik olarak o “scada” sistemlerinde dönme hızının yavaşladığını gösteriyor operatöre, ama aslında hızlanıyor ve orada 5-10 kişinin de ölümüne yol açmış galiba ve nükleer zenginleştirme programını 2 sene geri attığı da söyleniyor. Basitçe siber uzayda siber silahlar, gerçek hayatımızda etkisini görüyoruz.

Bu staks.net’ten sonra bu bilgi toplama, PRISM olayından bahsetmişti arkadaş, milyonlarca insanın izlenmesi ki, büyük veri, kafamızda bir şey oluşturmayabilir. Evet, “big data”; “Biz ‘big data’da neyiz?” Bir örnek vermek istiyorum: İsrail, özellikle kendi toprakları içinde bir türlü istediği insanları yakalayamıyor. Ne yapıyor, biliyor musunuz?



İnsanların davranışını incelemeye başlıyor ve su tüketimlerini toplamaya başlıyor. Evlerdeki su tüketimlerinin ani artışını, uzun süreli artışı, o eve bir misafir geldiğini gösteriyor ve periyodik olarak bunların datalarını toplayarak bunlar arasında bir korelasyon, bir örüntü kurmaya çalışıyor ve bazı kaçakların yerini böyle tespit edebiliyor. Basitçe ne yapmış oluyor aslında; su tüketim verisinden bir askeri operasyona vermiş oluyor. Kaldı ki ziyaretimize gelen Amerikan başkanları vardır. Bakanlarımızın elini de kontrol etmişlerdi, tek tek



bakmışlardı. Başkan, tuvaletini yanında getirmişti, tuvaletini bile koymuştu, beraberinde götürmüştü.

Ben başıma gelen şahsi bir şeyi anlatmak istiyorum: Bir tane kurumdayız, bir toplantıdayız, İsrail'den gelen bir delegasyon var. Çay getirdik, içmediler; kahve getirdik, içmediler, meyve suyu içmediler. Su getirdik, kendi ceplerinden, çantalarından su çıkardılar, içtiler. Çöpü de atmadılar, toplanırken de “Onu da bırakın” dediler, çöplerini de alıp gittiler. Yani dervişin fikri neyse, zikri de odur; Mısır'da bile idrardan bakıp adamın hasta olduğunu söyleyebilmişlerdi.

Peki, bu kapsamda bilgi güvenliğinin durumu böyle vahim, güvenilir



bilgi tamamen bu dezenformasyon ve maalesef ki manipülasyon sayesinde kime güveneceğimizi de şaşırdık. Her kaynak bizim için güvenilir bilgi vermemeye başladı. Devlet -ki en çok ben buna üzülüyorum- kurumlarımıza, hukukumuzda güven kalmadı, istatistik kurumlarımıza güven kalmadı. Yani yanlış anlamayın, ama yakında *“Kırmızı ışıktadır”* deseler, insan şöyle bir düşünüp *“Bir gidip İnternette araştırırım, harbiden kırmızı ışıktadır mıyız”* diye bakacak hale geldik.

“Sadece bizim ülkemizde niye bunlar oluyor?” diye düşünürsek, aslında dünyada da bunlar oluyor, ama biz maalesef ki şu an başroldeyiz, dünya sahnesinin önündeyiz. Sanırım dünyadaki büyük oyuncular, bu bölgedeki yaptıkları operasyonların sonucunda kim kazanırsa, o olarak çıkacak. Biz de bunun ceremesini çekiyoruz diye düşünüyorum.

Basitçe bilgi güvenliğiniz yok, güvenilir bilginiz yok, buna göre önleminizi alın. Çok basit bir önlem: Başkasının eline geçmesini istemediğiniz bilgiyi, ürettiğiniz içeriği -resim, yazı, müzik, her neyse, sadece onlar sizin- koymayın, bu kadar basit. Yani *“Arkadaşınız görsün, Ahmet görmesin”* diyeceğiniz bir resmi koymayın oraya; çünkü gün gelir, Ahmet de onu görür. Gerisi de zaten endişelenmeyin; çünkü sizin yapabileceğiniz bir şey yok. O yüzden biraz da rahat olun, böyle geldik böyle gideceğiz, hadi bari zevkini çıkarmaya bakın diyorum. Hani amiyane tabirle, tecavüz kaçınılmazsa zevkini çıkarmaya bakmak lazım.

Benim söyleyeceklerim bunlar. Sorularınız varsa, alabiliriz.

OTURUM BAŞKANI- Teşekkür ediyoruz.

Son birkaç yıldır özellikle TMMOB ve bağlı odaları, barolar, meslek örgütleri, sürekli iktidarların hedefindedir. Son olarak, 2 odamızda böcek tabir edilen dinleme cihazları çıktı. Bunların bir tanesi çok amatörce bir masanın altında, diğeri birazcık daha profesyonel



yapılmıştı. Böyle olunca, biz hep kendi aramızda da böyle konuşmalarımızda falan “*Bizim sakladığımız, gizlediğimiz bir şey yok, ne söylüyorsak zaten kameraların önünde söylüyoruz, panellerde söylüyoruz, raporlarımızda söylüyoruz. Hadi olur ya, insanız biz de, dedikodu yapıyoruz ara sıra, toplantılarda birilerini çekiştiriyoruz. Onlar çıkarsa, işte o zaman vahim, yani kimseye bakamayız*” falan diyoruz. Gerçekten Yasemin Hanım, oradan “*vahim*” dedi, söz geldi buraya, gerçekten vahim durumda.

Salondan soru sormak isteyen var mıdır? Toplu halde soruları alalım, ondan sonra konuşmacılarımıza hem eklemek istedikleri yerler var mıdır hem sizin sorularınıza cevap verecekleri yer var mıdır, ona dönüş yapalım.

Buyurun.

SALONDAN- Ben bir katkıda bulunmak istiyorum. Daha dün Ankara Şubede bir eğitim vardı, ISO 27001 VE 27002, bilgi güvenliği yönetim sistemi üzerine. Oradan yola çıkarak bir şey söyleyeceğim, yani bu karamsar tabloyu belki kendi açımızdan nasıl realize edebiliriz diye: Bir kurum, kamu ya da özel, fark etmez, bir bilgi güvenliği yönetim sistemi kuracaksa, ne türden tedbirler alması gerekiyorsa, ki bunun da birinci maddesi, o “*security*”nin politikasını belirlemekse, biz de kişiler olarak kendi “*security*”mizin politikalarını belirlememiz gerekir diye düşünüyorum. O açıdan da yerel “*network*”e ve yerel istihbarata daha hassas olduğu için karnımız, ne bileyim, Amerika’nın ya da başka bir ülkenin mail server’ını kullanmak bizim açımızdan çok sakat olmayabilir. Mesela Twitter şu ana kadar henüz daha bir şeyi paylaşmadı, herhangi bir şeyi vermedi diye biliyoruz.

ENGÜR PİŞİRİCİ- Ben o konuda bir düzeltme yapmak isterim: MIT’in son kanun tasarısına bakarsanız, bizim İnternet trafiği aslında çoğu yurtdışından geçer gider. Yani siz Facebook’ta arkadaşlarınıza mesaj attığınız vakit, aslında bir yurtdışına gider gelir. MIT, kuruluş kanunu çerçevesince yurtdışı bütün faaliyetleri, artı telekomünikasyon

faaliyetlerini izinsiz dinleyebilecek. Bu ne demek; kullandığınız e-postalar olsun, sosyal mecralar, şunlar bunlar olsun, aslında yurtdışı örnek göstermekle beraber, yine kendi vatandaşını hukuka dayanmadan dinleyebilecek.

Bir de ISO dediniz. ISO düzgün anlaşılmazsa, -önce insanda başlıyor, ISO çalışmalarında çok bulundum- evrak karmaşasına ve yığına



yol açıyor ve düzgün kullanılmıyor. En başta insanda farkındalığa ihtiyacımız var, yani politikadan da önce insanlarda bir farkındalık oluşturmak lazım. Eğitim şart.

SALONDAN (Devamla)- Ben şu açıdan söylüyorum: Yerel bir mail server, mail hizmeti sunan yerden hizmet almaktansa, gidip Gmail'den almayı tercih ederim.

ENGÜR PİŞİRİCİ- Snowden'in dokümanlarında NSA bir tane sanki dükkânmış gibi, satış pazarıymış gibi bir katalog yayınlıyor. O kataloga İnternette bakmanızı tavsiye ederim. Diyor ki, *"HP sunucular için bios'una yerleştirilecek virüs, del.ex sunucular için IPMI diye bir kısım var, ona yerleştirilecek virüs, şuna yerleştirilecek virüs,*



buna yerleştirilecek virüs...” Siz mesela operasyon yapacak bir CIA elemanısınız ya da NSA elemanısınız, o katalogdan istediğinizi seçiyorsunuz, yoktan var ediyorsunuz.

Yani yanlış anlamayın, ama İnternette coğrafi özellik kalmadı, onu önce bir çizelim. Türkiye sınırları diye bir kavram yok. Bilgisayarı biz üretmiyoruz, “*mainboard*”u biz üretmiyoruz, içindeki “*chip*”i biz üretmiyoruz. Mesela Almanya’nın federal hükümetinde “*chip*”leri analiz ederek, ters mühendislik uygulayarak analiz ederler, bakarlar olabildiğince, o da anlaşılır mı, anlaşılmaz mı? Bizde böyle bir kurum dahi yok. Geçiyorum, bu “*Open SSL bug*”ı, dünyanın gözü önünde, tamamen kaynak kodu açık bir şeydi, buna rağmen bu tip hatalar öne çıkıyor. Yani bizim üretmediğimiz, bizim lego gibi birleştirmedığımız şeylerin üstünde, sadece Türkiye’de kalsın dersek, belli bir kesimi zengin etmiş oluruz. Biz 3 dolara alabileceken o metaa 30 dolar ödemiş oluruz ve yine de kaptırırız, yine de ruhumuz duymaz.

SALONDAN (Devamla)- Ben onu söylemiyorum, ben kişisel olarak söylüyorum. Benim kişisel mail’im NSA’in ya da CIA’in ilgi alanına girmez. Belki bir yerde saklarlar, ileride bir şey olursam, bir aşamaya gelirim, kullanırlar. Ama kalkıp Yandex mail’i kullanmak istemem. Neden? Yandex mail’in Türkiye’de kurumsal yapısı var, tepesinde de Aydın Doğan’ın damadı var, istediği an her türlü bilgiyi oradan alabilir. Eğer Twitter ya da Gmail Türkiye’de ofis açarsa, onları da kullanmam. Ben bunu bir vatandaş olarak söylüyorum; çünkü bunu biliyoruz, yani istedikleri her türlü bilgiyi her yazdıklarını pat diye alamıyorlar.

ENGÜR PİŞİRİCİ- Birincisi, büyük veri için size de ihtiyacı var. Büyük veri için kesinlikle “*Beni ne yapsınlar?*” diye düşünmeyin, size de ihtiyaç var. Hatta bir İngiliz vatandaşının başından geçen bir şey var; GSM operatörü hakkında bir dava açıyor, diyor ki, “*Benim hakkımda tuttuğun bilgileri bana ver; verileri değil, bilgileri.*” En son kazanıyor. Adamlar sadece GSM sinyallerinden ve kimle konuştuğu, ne konuştu değil, kimle konuştu, kaç dakika konuştu ve baz istasyonundan



topladığı verilerle ne bilgiler üretmişler; hangi yolculuğu tercih ediyor, hangi firmayı tercih ediyor, nerelerden alışveriş yapıyor, kimlerle geziyor, kimlerle yatıyor, kimlerle kalkıyor, bilmem kaç CD çıkarmışlar... Sonuçta bilgisayar programları bunu işliyor, geçiyor. Onun için size de ihtiyaç var, “*crud database*”, “*big data*” için size de ihtiyaç var.

Diyorsunuz ki, “*O onun damadı, bu bunun bir şeyi.*” Tekrar söylüyorum; o aletler bizim olmadığı sürece, hepsi kandırılabilir olur, hiçbir vakit “*Şu güvenlidir*” diyemeyiz. Kanunen bazı şeyler var; mesela Sağlık Bakanlığı’nın şeyi şudur: “*Verileriniz dışarıda durmayacak, yani dışarıdaki bir data center’da durmayacak, Türkiye’deki data center’da tutacaksınız*” diyor.

SALONDAN- Kime diyor bunu, hizmet mi alıyor?

ENGÜR PİŞİRİCİ- Sağlık bilişim sektöründe hizmet veren firmalara.

SALONDAN- Bu konuyla ilgili çok güzel bir örnek vereceğim: Geçenlerde cep telefonundan arandım, ad ve soyadı olarak aranıyorum. “*Buyurun, benim*” dedim. Sigara bıraktırma konusunda bir şeyler anlatmaya başladı. “*Kardeşim, beni nereden buldunuz? Üstelik adımla arıyorsunuz?*” dedim. “*Bunu Sağlık Bakanlığı’ndan alıyoruz*” dedi. Sağlık Bakanlığı, bilmem kaç milyon insanın sağlık verilerini sattı.

ENGÜR PİŞİRİCİ- Bunlar biraz da avukatların suçu diyerek avukat arkadaşımıza bakayım. Bir tane program yazmışlar, 2004-2006, 45 milyon kişinin isim, soy isim, TC kimlik numarasını kasetlemiyorum sadece, nüfus cüzdanı örneği, oturduğu adres, seçmen kütüğündeki her şeyi koymuşlar, bir veritabanında toplamışlar, bunu icra avukatlarına satıyorlardı. Çünkü icra avukatı adres tespiti yapmakta zorlanıyor; siz “*Şu adam*” diyorsunuz, adam evini çıkartabiliyor.

Peki, bu programı satanlara ne oldu? El altından kullandırdılar, bir



şey olmadı; programı satmaya başladılar, bir şey olmadı. Avukatlar alıyor, düşünün. Sonra bunlar programın reklamını vermeye başladı, o zaman bizim devlet uyandı, “*Bir saniye, bu neyin reklamını veriyor?*” dedi, o zaman yakalandı, kolluk kuvveti o zaman operasyon yaptı. Bu benim de elime geldi. Ben kimim; hiçbir şeyim. Yani benim elime gelebiliyorsa, bilin ki o veride muhtemelen sizler de varsınız, herkesin elinde sizin TC kimlik numaranızı kastetmiyorum sadece, nüfus cüzdanınızın seri numarasına kadar bilgi sokakta geziyor. Türkiye, ürettiği verileri bir o kadar da kaptırıyor. Çok fazla veri üretiyoruz ve onları çok güzel kaptırıyoruz ve maalesef ki bunlara herhangi bir cezai şey de gelmiyor. Maşallah bütün dünyaya açıldık, bunu söyleyebilirim. Açık istihbarat yapan, bütçesi 2 bin dolar olan bir firma bile, çok rahatlıkla bizim birçok şeyin şeyini oluşturabiliyor.

OTURUM BAŞKANI- Buyurun.

SALONDAN- Ben bir soru soracağım, ama kim cevap verecek, bilmiyorum. Bu Ortadoğu coğrafyasındayız, Amerika bütün ülkeleri izliyor. Almanya Başbakanı Merkel’den özür diledi mi, dilemedi mi, bilmiyorum ama tepki koydular Almanlar ve Fransızlar. Türkiye’de hiçbir tepki yok.

ENGÜR PİŞİRİCİ- Açıklama dahi olmadı ki...





SALONDAN (Devamla)- Açıklama da yapılmadı, hiçbir şey yapılmadı.

ENGÜR PİŞİRİCİ- Yani politika olacak, ama “eşbaşkanıyım” diyordu, onu bir hatırlatayım.

SALONDAN (Devamla)- Ama hiç tepki koymadı Türkiye olarak.

Çin mühendisleri ve şirketleri, son 10-15 yılda Türk Telekom’un içinde çok çalıştı. Çin ve Rusya Türkiye’yi de izliyor mu Amerika gibi?

ENGÜR PİŞİRİCİ- Çin’in 2 büyük firması var, bunlar Türk Telekom’un NGN altyapısını falan yapıyorlar da kovuldular çeşitli yerlerden, Amerika’dan falan kovuldular. Bahane olarak da çok iğrenç bir bahane gösterildi; “ulusal güvenlik.” Yani affedersin de sen yıllarca ne yaptın da onların yapmasını bekliyorsun; hayır, ulusal güvenlik falan değil, basitçe ticaret. Dünya Ticaret Örgütü’nün kurallarını hiçe saymamak için böyle bahaneler uydurdular. Çin, öyle fiyatlarla piyasaya girdi ki, bu Batı bizim üstümüzden, hani bir koyundan 10 post çıkartıyordu, Çin sayesinde bunu engeller hale geldi dünya, ama Çin’i de böyle def etmeye çalışıyorlar. Verdikleri bazı fiyatları biliyorum, yani komple sistemin belli bir kısmının denetimi, o sistemin kurulumundan daha pahalıya geliyor falan. O yüzden “Çin de dinler mi?” Yanlış anlamayın da Çin niye dinlesin? Zaten 1 küsur milyar nüfusu var, eninde sonunda dünya onun hâkimiyetine girecek.

Tekrar altını çiziyorum: Çin’in bir küsur milyar nüfusu var diyorum. Mühendisiz, küsurat diyoruz, orada kaç Türkiye nüfusu var; 4-5 tane Türkiye nüfusunu biz küsurat yapıyoruz, mühendis olarak önemsiz diyoruz. O yüzden Çin, eninde sonunda kazanacak, onu söyleyeyim. O yüzden dinlemesine gerek yok. Niye dinlersiniz; bir amaç olması lazım. Amerika’nın amacı var. Amerika dünyada birinci sıraya nasıl oturdu? Bir insan, bir toplum, bir ülke, o pozisyona nasıl geldiyse, öyle koruyabilir o pozisyonu, bu çok önemli. Çin, zorlukla, silah gücüyle bir numaraya oturmuyor ki, ama bir yandan da Amerika’yı da çatır çatır dinlemiş, o da bir başka günün konusu olsun.



Bu siber güvenlikte bir kavram var, yeni yeni gündeme geliyor, gelişkin kalıcı tehditler diye geçiyor. Çin, öyle bir casusluk şebekesi kurmuş ki İnternet üstünden, 5 sene boyunca azar azar Amerika'nın birçok firmasından veri çekmiş ve onlarda da şu an Çin ataklarda bulunuyor, muhtemelen birçok teknolojiyi de araklamış diyoruz. AR-GE neydi; “*araştır-geliştir*”in dışında, “*arakla getir*”, onu da söyleyelim. Utanacak bir şey yok, “*arakla getir*” de çok rahatlıkla oluyor...

SALONDAN (Devamla)- Rusya ile Amerika, Kırım ve Ukrayna üzerinden bir sıcak savaşa doğru da gidebilir ya da anlaşır, bölerler, parçalarlar; Ortadoğu'ya da sıçrayabilir, Suriye üzerinden hesaplaşabilirler. Yani Türkiye yine ortasında kalıyor, bir Karadeniz'de, bir Akdeniz'de.

ENGÜR PİŞİRİCİ- Clinton'ın sözü vardı, “*21. Yüzyılın anahtar ülkesi Türkiye*” diye. Hatırlatırım.

OTURUM BAŞKANI- Toplu halde soruları alalım; çünkü diğer konuşmacılarımızın da söz hakkı olacak, karşılıklı olmasın.

Buyurun Yasemin Hanım.

YASEMİN- Bu kadar güvensiz bir ortamda bankaların sistemleri, onlardaki açıklar nasıl?

OTURUM BAŞKANI- Var mı başka sorusu, katkısı olan arkadaşımız? Yoksa, yine aynı sıralamadan hem eklemek istediklerinizi hem de diğer sorularla birlikte de değerlendirirseniz cevaplarınızı...

Buyurun.

İZLEM GÖZÜKELEŞ- Öncelikle kaldığım yerden devam etmek istiyorum.

Şu Arap baharından sonra, Ortadoğu'daki birçok ülkenin hassas noktalarını öğrenmiş olduk. Ancak şöyle bir şey daha vardı: Aslında ava giderken avlandılar. Çin başta olmak üzere, birçok ülke, bunları



sattı, amaç da daha çok gözetleyenleri gözetlemektir. Böylece o ülke, mesela Türkiye kimleri gözetliyor, Türkiye'nin hassas noktaları neler, görmek amacıyla bilerek ucuza sattılar. Amaçları para kazanmaktan çok o bilgiyi edinmekti.

Teknoloji aslında bir mücadele alanı, İnternet de bir mücadele alanı. Çoğumuz İnternetin nasıl ortaya çıktığını biliriz; Rusya uzaya adam gönderdi, ABD bir şey yapacak, nükleer saldırılara karşı bağışık bir sistem yaratmaya çalışıyor. Herkes bunu bilir, savaşın sonucu ortaya çıktığını görür; fakat nasıl olup da İnternet farklı bir yönde evrildi, bunu sormak lazım. Bu kısım pek anlatılmaz. 68 kuşağına bakarsak, ABD'nin Vietnam'da savaşta olduğu dönemdir. O zaman birçok ABD'li genç, askere gitmemek için -Türkiye'de olduğu gibi- üniversiteye gelir. Hippie kültürü, oradaki muhalif kültür, o teknolojinin çıktığı yerde toplanır. Bir yandan teknolojiye muhalif amaçları için kullanmak isteyenler vardır... Mesela arkadaşlar şunu derler: *“Bir gün acaba mutfak masamızda bilgisayar olabilecek mi?”* O zamanlar o büyük bilgisayar, bürokrasiyi, büyük araştırma kurumlarını, şirketleri temsil ediyor.

Bir grup hacker, *“Acaba masamızda bilgisayar olacak mı?”* diye düşünmeye başlar. O zaman Intel, ilk işlemciyi yaptığında şunu düşünmektedir: *“Bu işlemciler sadece trafik işleri gibi yerlerde kullanılacaktır”* ya da IBM, *“Adam bilgisayarını ne yapsın evinde?”* diyebilmektedir. Ama hacker dediğimiz insanlar, *“Acaba masamızda bilgisayar olabilecek mi?”* derler, çalışmaya başlarlar. Amaç, o büyük şirketlerin, devletlerin egemenliğini kırmaktır. Böylece o bürokrasiyi temsil eden büyük bilgisayarlardan daha âdemi merkezîyetçi teknolojiye doğru bir kayış olur. Bu oradaki muhalif kültürün bize sağladığı bir şeydir. Yoksa devletlere ya da araştırma kurumlarına kalmış olsaydı, dar şekilde gelişebilirdi.

Az önce sosyal medyadan konuştuk. Oradaki bilgilerin sahibi siz değilsiniz. Facebook kullanıyorsanız, Facebook'ta bilginin sahibi



siz değilsiniz. Ama hacker kültürü, hacker mücadelesi halen devam ediyor. Nasıl ki geçmişte âdemi merkezietçi yapı savunulduysa, ucuz bilgisayar kurmak için mücadele edildiyse, şu an aynı mücadele sosyal ağlarda var. Merkezi, tek bir yer yürütülen sosyal ağlar yerine, daha âdemi merkezietçi sosyal ağlarımız var. Bu sosyal ağlarda verinin sahibi sizsiniz. Bir gün başka bir şey kapanırsa, başka bir şeye gidebilirsiniz, daha bağımsız bir şey ya da e-posta iletişimi daha güvenli yapabilirsiniz...



Şöyle düşünün: Biz e-postayı güvenli kullanamıyoruz, e-postamız izleniyor. GnuPg e-postanın izlenmesini engellemek için yapılan bir yazılım. Biz bunu kullanırsak ve İnternetin o âdemi merkezietçi yapısını eğer ayakta tutabilirsek, bu mücadelede öne geçmiş oluruz. Sonuçta bir nokta giderse İnternette, İnternette bir şey olmaz; çok sayıda noktayı ele geçirirseniz, İnterneti çökertebilirsiniz. Biz İnternetin merkezietçi yapısıyla mücadele edersek, şirketlerden ya da devletlerden bağımsız şekilde, bu mücadeleyi kazanırız diye düşünüyorum, yani o kadar da kötü bir durum yok.

OTURUM BAŞKANI- Teşekkür ediyoruz.



Buyurun.

Av. YELDA GİZEM ÜNAL- Ben hem kısaca sorulara cevap vermek istiyorum hem de birkaç şey eklemek istiyorum.

5651 sayılı Yasa değişikliği şubat ayında sanıyorum kesinleşti. Yasa değişikliğinde herkes, bütün STK'lar, barolar, biz de dâhil, yasanın bu şekilde değişmemesi için bir sürü hukuki süreç de izledik, ama sonuç olarak değişti. Değiştiğinde, onların şöyle bir gerekçeleri vardı: *“Kişisel güvenliği sağlamak, kişisel veri güvenliği.”* Avrupa Birliği'nin ilgili sözleşmesinde trafik bilgilerinin 6 aydan 2 yıla kadar saklanacağıyla ilgili bir veri vardı. 2 ya da 3 gün önce galiba -bizdeki yasa artık Resmi Gazete'de de yayımlandı, zaten onun üzerine siteler kapatıldı- Avrupa Birliği, sözleşmesini değiştirdi, trafik verilerinin 2 yıl saklanması durumunu ekarte ettiler.

Ben de açıkçası durumun o kadar vahim olmadığını düşünüyorum. Gerçi İnternet ve teknoloji çok hızlı yürüyor, hukuk çok geriden geliyor, dolayısıyla birebir çareler bulunamıyor ne yazık ki, ama yine de çok vahim olduğunu düşünmüyorum. Dün TELKODER'in BTK'nın dinlemeleriyle ilgili; dinlemelerin içeriklerinin kayıt altına alınmamasına ilişkin başvurusundan yürütmesinin durdurulması kararı çıkarıldı. Mesela bu kararla birlikte, Avrupa Birliği'nin sözleşmesindeki 2 yıl verilerin trafik bilgisinin saklanması değişikliğiyle de birlikte, bizim her ne kadar *“Kişisel veri güvenliği yüzünden 5651'i değiştirdik”* gerekçesi olsa da bunun biraz daha ben iyiye doğru evrilmeye başlayacağını düşünüyorum. Başbakan, *“Kanunu değiştirdik, hadi yapın, Youtube'dan kaldırın, tape'leri silin”* dedi. Orada her ne kadar kişisel veri güvenliği dese de, bir ay kadar önce başka bir yerde bir seminerde şey dediler, *“Kişisel veri güvenliği nedir, neyi koruyor?”* Kişisel verilerden para elde edilen bir ortamda, kişinin veriyi koruması gerekçesiyle yasanın değiştirilmesi söz konusu değil. Bunun birazcık politika olduğu aşikâr, zaten iktidar da bunu dolaylı yollardan ikrar etti. Dolayısıyla bu sözleşme değişikliğiyle de birlikte öyle sanıyorum



ki yerel seçim oldu, Cumhurbaşkanlığı seçimi olacak vesaire, kısa bir süre sonra da yeniden bu yasaların değişeceğini düşünüyorum, zaten çok hızlı bir şekilde değişiyor biliyorsunuz.

Onun haricinde, az önce konusu geçti, ama tam ne şekilde geçti, hatırlamıyorum, kriptolu telefonu Başbakanın kullanması olayı. Kriptolu telefon kullanılması, 5809 sayılı Elektronik Haberleşme Yasası'nda belli sayıda kişinin kullanımına açılmış bir durum, bunlardan bir tanesi Başbakan değil. Dolayısıyla resmi, gayet legal bir şekilde “*Kriptolu telefonlarımızı dinlediler*” gibi bir cümlenin kabul edilebilir yanı çok yok; çünkü zaten kriptolu Başbakanın kullanıyor olmasının, yasada en azından karşılığı yok. Tabii bazı şeylerin yasada karşılığının olması ya da olmaması, Türkiye’de hukuksuz olduğu ya da olmadığı anlamına net olarak gelmez..

Bir de siz dediniz, “*Melih Gökçek 150 bin dolarlık bir güvenlik ağı kurdu*” diye. Belediyeye mi, kişisel mi, bilmiyorum, güvenlik duvarı örmüş. Bunun üzerine hacker’lar şey diyorlar, bir sürü İnternet sitesi var şimdi, gerçi geçtiğimiz aylarda bir tanesi kapatıldı, bu İnternet sitelerindeki açıklarla ilgili bir ödül sitesi kurulmuştu 5 ay kadar önce. Açığı buluyorsunuz, onu rapor ediyorsunuz, ama kesinlikle kötüye kullanmıyorsunuz. Bu şartlar altında site, devlet kanallı bir site olmamakla birlikte, size ödül veriyor. Ancak yürümedi; çünkü hacker’ların bilmiyorum gelirleri nedir, ama o sitedeki ödülü almaktansa, onu hack’leyip daha büyük bir popülasyona hitap etmeyi tercih ettiler. İnternet güvenliği böyle iken hacker ın dediği gibi “*İnsanlar hâlâ Greenpeace’in dünyayı kurtaracağını sanıyorlar, ama öyle olmayacak; sıfırlar, birler dünyayı kurtaracak.*” Öyle bir zihniyetleri var.

Teşekkür ederim.

OTURUM BAŞKANI- Teşekkürler.

Buyurun.



ENGÜR PİŞİRİCİ- Benim elimde iki tane hap var; biri kırmızı hap, biri mavi hap. “*Mutlu mutlu yaşayalım*” demeyeceğim, ben maalesef ki size kırmızı hapı öneriyorum.

Başlayalım, mesela Arap baharından başladık, Arap baharından bahsettik. Arap baharının kendinden gerçekleştiğini mi zannediyorsunuz? O zaman belli kivotleri vereyim, eve gidince bir bakarsınız. HP geri, Amerikan Hava Kuvvetleri ve personel yazılımı. Bu kivorte baktığınız takdirde şunu görürsünüz: Bir Amerikan askeri projesinin deşifre olmuş hali. Askeri proje şunu içeriyor: Sosyal mecra yönetim programı. Bu ne demek? Sosyal mecralarda sayıları 100 binleri bulan feyk karakterler yaratılıyor ve yaşıyorlar sosyal mecrada.

Mesela Mısır’da 15 bin tane karakter yaratıyor bu program ve bunu tek kişi yönetiyor. Bu seçimlerde gördüğümüz gibi, birebir aynısı “*copyface*”yle troller, Twitter’lar gibi değil de gerçekten birbirleriyle konuşan, muhabbet eden, yerel zamanındaki gibi yaşayan, iş sahibi gibi gözüken, arkadaşları var gibi gözüken, çeşitli fotoğraflar paylaşan, basitçe sanal ortamda karşıdakini gerçekmiş gibi çizen bir yazılım. Siz böyle bir yazılımla sosyal medyaya hükmettiğiniz takdirde, 10 bin kişi “*Hadi meydana toplanıyoruz*” derken, aslında sadece 9 bin tane feyk karakter, 5 kişi “*Hadi meydana gidiyoruz*” derse, diğer insanlar da gelmeye başlayacaktır. Biraz düşünelim, aslında Arap baharının o kadar da masumane olmadığını görebiliriz. Sağ olsunlar, aynı zamanda iyi doküman sızdırıyor Amerikalılar.

Arkadaşımız bir şey söyledi, güzel bir noktaya değindi, ama ben orada bir düzeltme yapmak istiyorum. İnternetteki içeriğin sahibi sizsiniz, ama kontrolü sizde değil. Kontrolünün sizde olmadığı gerçeği, sahibinin siz olmadığı anlamına gelmez; sahibi sizsiniz, ama kontrolü sizde değil.

Trafik bilgileri konusundan bahsettik, “*Güzel günler bizi bekliyor*” dedik. Ben bir soru sorayım: Trafik bilgileri nerede tutuluyor; elektronik ortamda. Soruyorum: Elektronik ortamda tutulan verilerin



nasıl silineceği konusunda bir tane mevzuatımız var mı? Evrak imhası konusunda mevzuatımız var, adamlar diyor ki, “6 aydan az, 2 yıldan fazla olmamak üzere -‘ki yenisinde galiba bu 6 ay uzadı aslında’- saklayacaksınız.” Ne yapacak, mevzuat var mı; yok. Sadece silip mi geçeyim, mutlu mu olayım, yani sadece *delete* tuşuna basıp silersem, o veriler, o bilgiler silinmiş mi olacak, yoksa bunun aslında bir mevzuatının olması gerekmiyor mu sizce? Yurtdışında, Amerika’ya yeniden keşfetmeye gerek yok, elektronik verilerin nasıl silineceği, nasıl imha edileceği konusunda tonla belge, bilgi, doküman, mevzuat, kanun, her bir şey var, ama Türkiye’de bunlardan bir tanesi yok. Buna rağmen böyle bir yasalar zincirimiz var. Hadi bakalım, herkes kafasına göre “yok etsin.”



Mesela çeşitli firmalar, “*bug band*” dediğim programı

yapar. Bu ne demek; siz Google’a düzgün şartlarda -ki onların belli şeyleri var, şartlar oluşmuş zaten- bir bulduğunuz açığı bildirirsiniz, ona göre önlem alır, ona göre sizin isminizi geçirir, ona göre de belli bir para verir. Bunların yarışmaları da olur, yani “*white hacker*” dediğimiz, beyaz şapkalı hacker’lar aslında piyasada bayağı bir dolaşiyor. Artık bu iş gönüllü olmaktan çıktı, ya devletlere satıyorlar; mesela bir fiyat söyleyeyim: IOS 7.1. için yayınlanmamış bir “*exploit*” bulursanız, sömürülecek bir nokta bulursanız, bunu yaklaşık 200 bin Avro’ya çok rahatlıkla satabilirsiniz, varsa elinizde.

Bankalarda güvenlikle ilgili bir soru geldi. Normalde Türkiye’de bunun herhangi bir altyapısı oluşmadan, bir “*penetration testing*”



kavramı çıkmadan, bankaların zorunlu olarak bir sızma testi yapmaları şart koşuldu. 20 küsur tane banka var, çok pahalıya yaptırıyorlar. “*Penetration testing*” zafiyet taraması değildir, ama maalesef Türkiye’de bunu yapıyorlar daha çok. “*Penetration testing*”i anlamanız için en güzel örnek, 92 idi galiba yapımı bir film, “*Snickers*” diye, orada bankaya “*penetration testing*” yapıyorlar harbiden. Geceleyin giriyorlar, içeriden iki tuşa basıyorlar, dışarıdan da bir iki tuş, sonra bir parayı başka hesaba aktarıyorlar falan... Eğer bulursanız, o filmi muhakkak izlemenizi tavsiye ederim. O yüzden Türkiye’deki durum da bankalar açısından pek iç açıcı değil. Ancak banka müdürü bir tanıdık var, amiyane tabirle şöyle söyledi: “*Bizim bankada 200’den fazla avukatımız var, burası da söğüt gölgesi değil, gitsinler, dava etsinler.*”

Sonuç olarak şunu söyleyeceğim: Her ne kadar güvende olduğumuzu hissetsek de tekrar söylüyorum, bu bir tiyatrodur, güvenlik tiyatrosudur, güvende olmakla güvende hissetmek ayrı şeyler. Hangi hapı alacağınız; kırmızıyı mı, maviyi mi, size kalmış.

Teşekkür ederim.

OTURUM BAŞKANI- Çok teşekkür ediyoruz.

Aslında bu konu, hem dediğimiz o teknoloji düşmanlığı vesaire, onun dışında, keyifli ve aslında sürekli devam ettirilmesi gereken bir şey. Bunu bildiğiniz gibi, Bilgisayar Mühendisleri Odası ayrılmadan önce, bilgisayarlılar aramızdayken Ağ ve Bilgi Güvenliği Sempozyumu düzenledik, 2’şer-3’er gün sürerdi; o için hem teknik boyutunu hem sosyal boyutunun, politikalarının belirlendiği sempozyumlardı. Dördüncüsünü sanıyorum 2011’de düzenledik. Oradan bu zamana 3 yıl geçmiş, bu ağ ve bilgi güvenliği konusunda daha çok yapılması gereken şeylerin de gündeme geldiğini ifade etmek gerekiyor. Umuyorum önümüzdeki yıllarda bu sempozyumun yeniden yapılması ve için çok daha farklı yönleriyle ele alınmasını hayata geçirebiliriz.



Konuklarımıza çok teşekkür ediyoruz, gerçekten değerli bilgilerini bizimle paylaştılar. Halil Ağabeyimizi saygıyla anıyoruz. Kendisi yaşıyorsa ve bizimle birlikte olsaydı, eminim bu sıralarda birlikte olacaktık, dinleyecekti ve belki de öfkeli bir şekilde sorusunu soracaktı. Türkiye’de şu anda birçok arkadaşımız, bu yaşananlara yönelik olarak, ortamda bu kadar inandığı bilgi varken, yoğunluğun da inanmadığı bir bilgi varken ortada, toplum tamamen kutuplaşmışken, hem öfkeyi barındıran cümleler kuruyoruz hem de beraberinde başka refleksleri bekliyoruz. Biz yine umutlu bir şekilde kapatalım panelimizi. Umarım güvenli bilgiye ulaşabileceğimizi, güvenilir bilgiye ulaşabileceğimiz mecraları daha da artırırız ve gerçekten sağlıklı bir şekilde bu süreci kurtarırız diye düşünüyoruz. Katıldığınız için hepimize çok teşekkürler. İyi akşamlar.



aramızdan ayrılan EMO Ankara Subesi
Kurucu Yönetim Kurulu Üyesi Halil EKER anısına...



panel:

BİLGİ GÜVENLİĞİ ve GÜVENİLİR BİLGİ

10 NİSAN 2014 PERŞEMBE 18.30
EMO GENEL MERKEZİ TOPLANTI SALONU
İhlamur Caddesi No: 10 Kızılay Ankara

Oturum Başkanı:

Ebru AKGÜN YALÇIN • EMO Ankara Şubesi Yönetim Kurulu Başkanı


Panelistler:


İ. İzlem GÖZÜKELEŞ • Bilgisayar Mühendisi


Av. Yelda Gizem ÜNAL • Ankara Barosu Elektronik Haberleşme Hukuku Kurulu Başkanı


Engür PİŞİRİCİ • Bağımsız Siber Güvenlik Araştırmacısı

Necatibey Caddesi No:102/3 Maltepe, 06570 Ankara, Türkiye
Telefon: +90 312 231 44 74 Faks: +90 312 232 10 88 GSM: +90 530 773 09 37, +90 530 773 09 38
e-posta: ankara@emo.org.tr web: <http://ankara.emo.org.tr>

 /emoankara

 /groups/emoankara

 /emoankarasubesi

 /emoankara

