Son 20 Yılda Bilişim-Telekom Bize Çalıştı mı? Siber Güvenliğin Uluslararası Boyutları

Füsun Sarp Nebil - *turk-internet.com Yayın Yönetmeni*
fusun@nebil.com

Ortadoğu her zaman sıcaktı ama son 20 yıldır daha da hareketli. Önce Irak, sonra Suriye derken şimdi İran ile uğraşılan bir dönem var. 2019'da ABD'de vizyona giren "Official Secrets" filminde ABD-İngiltere'nin Irak savaşını nasıl "illa" haline getirdiği görülüyor[1]. Suriye konusunda başka şekilde "illa"lar oldu. Şimdi İran konusunda ne olacak ve daha önemlisi bize ne olacak?

İran için çeşitli yorumlar var. Benim saygı duyduğum yorumlardan birisinde Osman Başıbüyük, ABD'nin Orta Doğu'dan çıkışına, Çin'in bölgeye girişine ve ABD'nin Arap ülkeleri üzerinde hakimiyeti kaybetmemek kaygısına dikkat çekiyor[2]. Bu bir yorum. Ama bizim sektörümüz açısından bir şeyleri düşünüp, planlamamız gerektiğini de hatırlatıyor.

Aralık 2019 sayısında yazdığımız "Siber Güvenlik" makalesi ekim sonundaki Garanti Bankası uzantısında, ülkemizin durumuna bakıyordu. "Siber Güvenlik" denildiğinde, sadece bir takım virüsleri kullanarak bilgisayarlarda ya da sunucularda programların / verilerin bozulması ya da kilitlenmesi (ve fidye istenmesi) ya da botnetlerle yapılan dDos gibi bir takım saldırılar anlaşılsa da, bu kadar basit değil.

Siber güvenliğin düşünmediğimiz başka boyutları da var. Bu yazıda uluslararası kapsama dikkat çekmek istiyoruz. Ancak not olarak iletelim; burada anlatacağımız konular belli başlı bir kaç noktayı içerecek. Aslında çok daha fazla ilgilenilecek konu var. Biz sadece hemen önümüzde olan bir kaç konuya değineceğiz.

Bilişim Bize mi Çalışıyor?

Başlıktaki soruyu yazının sonunda yeniden soracağım !!! Çünkü % 80+'sı yabancı ürünlerle dolu bir bilişim-telekom sektörüne sahibiz.

II. Dünya Savaşı'nın bitimi sonrasında, soğuk savaş döneminde, casuslar çok moda oldu. Bu casuslar kendi hayatlarını tehlikeye atarak, diğer ülkelerin bilgilerini almaya çalışırlardı.

Ama yanısıra ABD, "5 Eyes" olarak bilinen "Yeni Zelanda - Avustralya - Kanada - İngiltere - ABD" müttefikliği ile başka bir tür casusluk da yapıyordu. Bu ülkelerde kurulmuş olan antenler ve çeşitli yerlerdeki kablo dinleme operasyonları (örneğin Güney Kıbrıs'taki İngiliz üssünden yapılan gibi), dünyanın bilişim ve iletişim teknolojilerini "casusluk" anlamında ilk kullanım yoluydu.

Ancak 1980'lerde bilgisayarlaşmanın artması ile birlikte, ortam değişti ve ülkeler bilişim - telekom yoluyla standardize edilmeye ve çok muhtemelen de kontrol altına alınmaya başlandı. Çünkü bilişim ve telekomda yerelleşme yok oldu, yerine bilişim, internet ve telekom devlerinin herşeyi kontrol altına aldığı bir dünya geldi.

Türkiye'nin de dahil olduğu ülkeler bilişim teknolojilerini, başka herhangi bir "arka plan" düşüncesi olmadan aldı ve kullandı. Ama acaba bilişim-internet-telekom bize çalışırken, başka şeyler de yapıyor mu?

Önemli bir soru bu !!! Bunu aşağıda anlamaya çalışacağız. Biraz tartışma ortamı yaratmak istiyoruz.

Açık Kaynak Olmayan Yazılımlar

1990'lı yıllarda yayınlanan Bilgi Mafyası isimli kitap çok ilginç detaylar içeriyordu[3]. 1980'lerde bir programcının geliştirdiği Promis adlı bir yazılım çevresinde dönen gerçek hayattan alınma hikayeleri, öldürülenleri filan okuduk. Bu kitapta, henüz internetin yaygınlaşmadığı yıllarda bile bilgisayarların istihbarat örgütleri (kitapta Mossad'dan bahsediliyor) tarafından nasıl kullanıldığına dair bilgiler veriliyordu.

Örneğin, Ürdün'ün başkenti Amman'daki su şirketine bir bilgisayar hediye edildiği anlatılıyor. İnternetin olmadığı günlerde, bu bilgisayarın bir kablo ile yakındaki eve bağlantısı kurulmuş ve oradan şehrin tüm su sarfiyatları izlenmiş. Herhangi bir evde su sarfiyat ciddi bir şekilde artınca da "Filistinli saklanıyor" diye o eve baskın yapılıp, "eliyle konulmuş gibi" saklanan kişiler yakalanmış. Saklananların nasıl keşfedildiği ise uzunca bir süre bulmaca olarak kalmış ve anlaşılamamış.

Dünya "Açık Kaynak (Open Source)" demeye ancak Netscape kaynak kodunun açıklanması ile 3 Şubat 1998'de başladı [3]. Linux da açık kaynak tarihinin önemli bir adımı oldu [4].

Açık Kaynak demek, **"ne iş yaptığını görebildiğiniz"** yazılım demektir. Ya da diğer deyişle, para vererek satın aldığınız yazılımın sizin işinizi yaparken, diğer yanda **başka bir yere de iş yapmamasını garanti altına almak** demektir. Sizin ya da şirketinizin bilgilerini aktarıyor mu acaba?

Şirketlerimizin ve devlet kurumlarımızın hemen hepsi son 30 yılda veri tabanı, işletim sistemi ve yazılım olarak çok uluslu ve de başta Microsoft, Oracle, SAP olmak üzere kapalı kaynak kodlu ürünler aldılar. Bu bir siber tehdit midir? Bilmiyoruz !!!

Örneğin, İran Ukrayna uçağını düşürürken 10 saniye kadar telefonlar çalışmamış. Uçağın bir füze olduğu sanılmış ve kontrol edilmeye çalışıldığında anlaşılamamış. Acaba burada Stuxnet olayında olduğu gibi, yazılımların içindeki sonradan eklenmiş ya da virüsle yapılmış bir operasyon var mıydı? 5-6 yıl sonra ortaya çıkacak bir siber saldırı var mıydı? Yazılımların içindeki gözükmeyen kodlar mı çalıştı? Şimdilik bilinmiyor.

Bilişim Ambargosu?

Kapalı kaynak yazılımların "içini görememek" dışında bir sorun da, lisanslı olmaları ve günümüzde ancak anahtar kodu ile çalışmaları. Bunun parasal yönü yani "pahalı" vs olması bir yana, asıl sorun günün birinde "artık kullandırtmıyoruz" şekline dönüşme olasılığı[6].

Bugünlerde örneklerini Adobe'nin Venezüela, Java'nın Rusya ve GitHub'ın İran, Kırım, Suriye'deki kullanıcıları bloklaması gibi örnekleri ile yaşadık. **"Bilişim ürünlerinde ambargo"** kullanılabilecek diğer bir **"siber silah"**. Hatta SAP kullanan firmaların yaşadığı gibi, birden bire "İran'la iş yapıyorsanız, bizim yazılım üzerinden yapamazsınız" gibi bir kısıtlama ile karşılaşmak da mümkün[7].

Özetle, parasını vererek aldığımız bu yazılımlar bir gün işe yaramaz olurlarsa, kullanmamız engellenirse, acaba ne tür bir komplikasyon yaşarız? Buna dair plânı olan var mı? Bu da önlem alınması gereken bir "Siber Tehdit" midir?

Böcek İçeren Ya Da Arka Kapıları Olan Donanımlar

Edward Snowden'in 2013 yılında sızdırdığı belgelerin bir kısmında Cisco isimli firmanın önemli yabancı kurumlara satılan cihazların içine böcek taktığına dair evrak ve fotoğraflar vardı [8]. Şimdilerde Trump "Huawei ürünleri casusluk yapıyor" diyor. Nereden biliyor acaba? Kendilerinin yaptıklarından mı?

Türkiye'ye giren bazı elektronik cihazların sağlığa etkileri --mesela cep telefonlarındaki SAR değeri-- gibi bazı özellikleri test ediliyor. Ancak bırakın şirketlerimize, devlet kurumlarına alınan donanım ve cihazlar için bile bir **"güvenlik kontrolü"** yapılmıyor. Buna dair bir düzenleme ya da kural yok.

Oysa, yıllar içinde bağımsız güvenlik araştırmacıları tarafından, hemen her cihazda "arka kapı" tabir edilen türden girişler keşfedildi. Juniper, Fortinet vs.. [9] Bu açıklar tespit edildiğinde, firmalardan "soruşturma açtık" sözleri duyuldu. Ama şimdiye kadar bu soruşturmaların sonuçlarını duyduğumuzu hatırlamıyoruz.

Bulut Hizmetleri

Bulut hizmetleri, bir kurum için çok faydalı gözüküyor. Hem maliyet, hem en son teknolojileri kullanmak, hem kolaylık vs. Düşünün, bilgisayar / sunucu sistemleriniz eskidikçe değiştirmek için tonla para vermekten kurtulacaksınız. Büyüyüp, küçülmeniz hızla mümkün. Hatta SaaS yani yazılımın bir hizmet olarak sunulduğu modelde, yazılıma da para vermiyorsunuz. Sadece aylık bulut kirası neyse onu ödüyorsunuz.

Buraya kadar adeta "Alaaddin'in Sihirli Lambası". Ama ya birileri sizin bu verilerinize yani mesela teklif dosyalarınıza ya da müşterilerinizin kimler olduğuna bakıyorsa? Örneğin Airbus için böyle bir tartışma olmuştu. Bir ihalede Boeing'in Airbus'a ait teklif kayıtlarını ele

geçirdiği konuşulmuştu. Tabi nereden olduğu tam bilinmiyor.

Türkiye'deki bankaların verilerinin yurt dışında depolanması, BDDK tarafından yasaklanmıştı. Sonra kişisel veriler kanununda benzer bir tanım yapıldı. Ama sonra pek çok noktada esnetildi. Şimdi soralım; çok uluslu bulut servisleri ne kadar güvenli? Ya da ambargo için bir araç olabilir mi?

Kritik Altyapılar

Uzun zamandır konuşulan bir konu da bu. Elektrik sistemi, ulaşım, su sistemleri gibi kritik altyapıların gözden geçirilmesi ve gerekli önlemlerin alınması gerekli. Örneğin İran'ın nükleer yakıt zenginleştirme sistemlerine 2007'lerde CIA tarafından yapıldığı açıklanan Stuxnet saldırısı, basitçe sistemin Siemens marka PLC cihazlarının ayarını bozmaya dayanıyordu [10]. Aynı şekilde skada sistemlerine saldırı bilinen bir şey.

Bugün bu konu çok ciddi. Bir ara Ankara'da bu konuda bir konferans düzenlenmişti. Ama o günden bu yana başka bir çalışma göremiyoruz.

Uydular ve Navigasyon (GPS)

Bugün cep telefonlarında kullandığımız GPS yani Amerikan Navigasyon sistemi, aslında askeri uçaklara yönelik bir konum belirleme sistemi idi. Zamanla sivil uçaklar ve sonra da cep telefonlarımıza kadar geldi. Ancak bu sistemin ABD hükümeti tarafından zaman zaman manipüle edildiği biliniyor. Bosna savaşında Avrupalıların, Güneydoğuda yapılan operasyonlar sırasında da ülkemizin bu sistemi kullanmaya yönelik sorunlar yaşadığı görüldü[11].

Navigasyon sistemindeki bir kaydırma ile pek çok uçak kazası ya da başka türlü sorun oluşabilir. O nedenle ülkemizin bu konuda sadece Amerikan GPS sistemlerine bağımlı olması doğru değil. Avrupa'nın Galileo sistemine dahil olması gerekirdi.

Uydu konusu sadece GPS açısından değil, alçak yörünge uydularından internet açısından da önemli. Elon Musk, Çinliler ve Amazon dünyayı uydu battaniyeleri ile sarmaya hazırlanıyorlar. Bunun amacı, nesnelerin interneti dünyasında gerekli olan interneti gökten sağlamak. Bizim burada geride kaldığımız ortada [11].

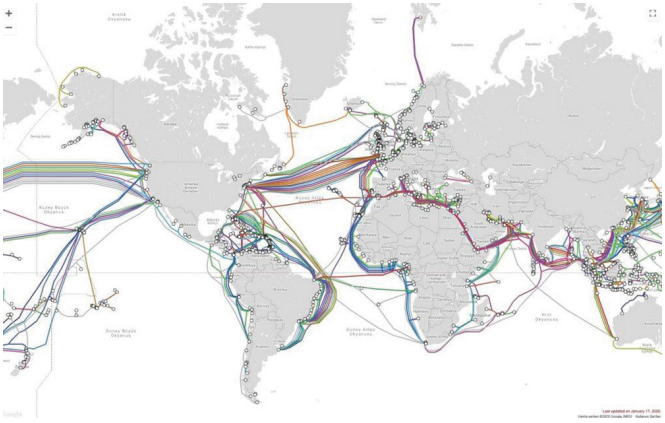
Türk Telekom ve Turkcell ile duopol halindeki telekom sektörünün, yaklaşan uydu battaniyeleri projeleri ile ne kadar hayatta kalabilecekleri de ayrı bir soru işareti.

Geleceğin uzaya alınmakta olduğunu bugün Elon Musk'ın, Çin'in hatta Hindistan'ın artan çabaları ile farkediyoruz. Uydu konusunda biz hala Türksat'ın boş durmakta olan TV uyduları atma motivasyonunu anlayamıyoruz. Bunun mümkünse internete ve navigasyona çevrilmesi lazım. Hindistan sadece kendi bölgesini kapsayan daha dar bir navigasyon sistemi kuruyor.

Denizaltı Kabloları

Nedense Avrupa'nın Ortadoğu ve Asya ile olan bağlantıları karasal değil. Yani karadan giden kablo hatları daha ucuz, daha kolay kurulabilir, daha kolay işletebilir olmalarına rağmen aşağıdaki haritada göreceğiniz üzere Avrupa'dan mesela Hindistan'a gidilecekse Akdeniz, Kızıldeniz, Arap yarımadası çevresinden, Hint Okyanusundan geçerek gidiliyor. Kulağını öbür elinle göstermek gibi bir şey.

Ya da biz Çin ile haberleşeceksek yine bu yol var. Ya da Avrupa, Atlas Okyanusu, ABD boydan boya, Pasifik Okyanusu, Japonya, Sarı Deniz ve Çin şeklinde bir deniz yolu kullanıyoruz. Oysa Hazar Denizi'nin altından ya da üstünden geçecek kablolarla daha kolay ulaşamaz mıyız? Ya da daha ucuz?



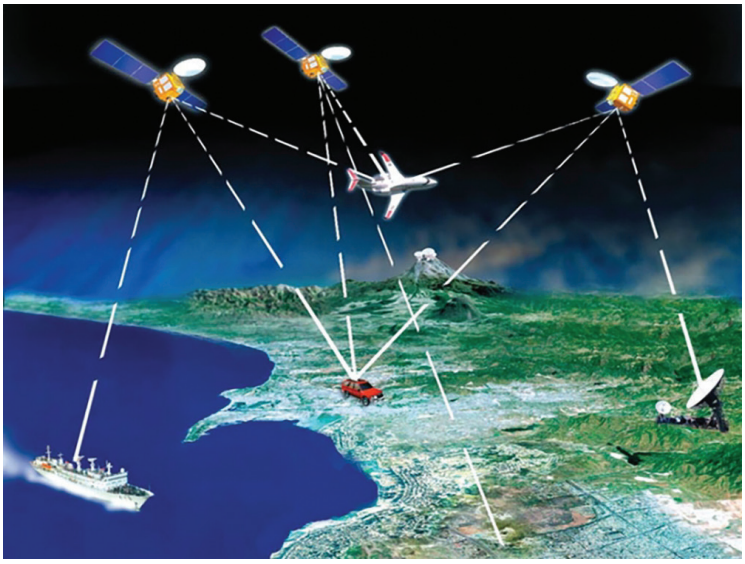
Yukarıdaki haritada sadece denizaltı kabloları yer alıyor. Ancak dediğimiz gibi Ortadoğu ve Asya bölgesini, Avrupa'ya karadan bağlayan hat yok ya da yok denilebilir düzeyde.

Aynı şekilde İnternet Trafik Değişim Noktası konusu var. 20 yıl önce kurulmuş olmalıydı ama yok. Çünkü bu da bölgeyi trafiğin geçtiği bir hale sokardı.

Peki bu neden böyle? İstanbul, Avrupa-Asya-Ortadoğu-Kafkaslar arasında bir doğal kavşak. Ama oyunun dışında kalmış. Çünkü oyun, kabloların içinden geçen veriler, bu verileri geçirmek için ödenecek paralar ve bu iletişim sistemini yönetmek için gereken knowhow birikimi ile çok önemli.

Biz mi? Uyuyoruz.. ya da uyutuluyoruz...

Yerel Sektörün Yokedilmesi ve Türkiye'de Bilişim Kime Yarıyor?



1990'lardan sonra yükselen bilişim sektörünün bugün geldiği kompozisyona bakarsak % 80+ yabancı firmalara yaradığı görülür. Yerli yazılım firması olan pek çok firmanın da aslında Microsoft gibi platformlar üzerinden hizmet verdiğini hesaba katarsak, sadece hizmet bedeli olarak alınan küçük bir rakam sektörün esas gelirini oluşturuyor. Bu nedenle de baktığımızda 20 seneyi aşan yerli firma sayısı çok az.

Aynı şekilde kıymetli ve ülkeye katkı yapacak olan bilgisayar ve elektronik mühendisliği gibi mezunlar da çok uluslu firmaların yüksek maaşlı satış kadrolarında dikey ve 10 sene içinde modası geçen konularla köreltiliyorlar.

Başta sorduğumuz soruya gelirsek? Türkiye'de Bilişim kime yarıyor? Kabul; verimlilik ve iş yapış usülleri açısından bize yarıyor. Ama bizden daha fazla başkalarına yarıyor olabilir mi? Parayı sormuyorum bile.

Yani, yerel bir bilişim sektörünün oluşamamasının nedeni sadece para mıdır? Bu oluşamamayı yöneten nedir? Bilişim ve telekom sektörünün mevcut durumu, maliyetini biz ödediğimiz halde, bizzat bize karşı bir siber tehdit içeriyor mu? Bunları hep birlikte sorgulamalıyız. Düşünmeliyiz.....

[Türk bilişim tarihini yazıyorum. Orada bazı noktaları anlatacağım]

Hepsi Bu mu?

Bu yazıda otonom silahlardan, böcek boyutundaki drone'lardan ya da gitgide daha fazla konuşulur hale gelen elektromanyetik silah ve bombalar gibi gerçekleşmiş ya da gerçekleşeceği düşünülen fantastik siber tehditlerden söz etmedik bile. Yani daha konuşulacak çok fazla konu var.

[1] Gazeteciliğin Önemi : Irak Savaşı Bush-Blair İkilisi Tarafından Nasıl Kotarıldı?

[2] İRAN'DA NE OLDU, ŞİMDİ NE OLACAK? | OSMAN BAŞIBÜYÜK | KARTAL-1

[3] Bilgi Mafyası Kitabı

[4] Open Source Initiative

[5] Wiki-Turk : Linux

[6] 2019 Ekim Dosyası : Bilişim ve Telekomünikasyonda Ambargo ve Yaptırım

[7] ABD İstedi, SAP Müşterilerine Benim Yazılımım Üzerinden İran'a Mal Satma Dedi

[8] Ortaya Çıkan Fotoğraflar NSA'in Cisco Cihazlara Casus Parçaları Taktığını Gösteriyor

[9] Juniper Networks Firewall'larında Arka Kapı Kodu Bulundu, FBI Olayı Soruşturuyor

[10] Zero Days Belgeseli

[11] Coğrafi Konumlama (GPS) Savaşlarına Bir Bakış

[12] Elon Musk'ın SpaceX Firması Uydudan İnternet için 500 milyon $ Fon Topluyor

EMO ANKARA ŞUBESİ SATRANÇ TOPLULUĞUNDA BULUŞALIM: EMOCHESSANKARA

EMOChessAnkara EMO Ankara Şubesi Satranç Topluluğu'dur. Satranca meraklı EMO üyelerini bir araya getirme amacıyla kurulan grup Lichess platfomu üzerinden düzenli aralıklarla online turnuvalar ve yüz yüze satranç buluşmaları, turnuvalar düzenlemeyi hedeflemektedir. Topluluk çalışmalarına katılmak isteyen üyelerimiz web sayfamızdan QR kodu takip ederek whatsapp grubuna katılım sağlayabilirler.