SİBER GÜVENLİK VE ÜLKELER

Ali Kurtul – Elektronik ve Haberleşme Mühendisi

Dünyada ve Türkiye'de hayatın bir parçası haline gelen siber dünya sadece bir hayat kolaylaştırıcı olmaktan öte bireyler, şirketler, kurumlar ve devletler için vazgeçilmez hale gelmiş ve bu vazgeçilmezliğin sonrasında bizleri bekleyen tehdit ve tehlikeler oluşmuştur. Artık teknoloji olmadan devletler çalışamaz, şirketler iş yapamaz ve bireylerde, hayatlarının ayrılmaz bir parçası haline gelmiş bu işlevler olmadan, hayatlarını devam ettiremez noktaya gelmiştir. Artık devlet bir taraftan sunduğu hizmetlere devam ederken, birçok stratejik bilgi ve planlarını teknolojik araçlar vesilesiyle saklamaktadır. Benzer şekilde şirketler de yaptıkları işlerle ilgili kritik bilgileri, müşteri verilerini, ticari sırlarını teknolojik araçlarla saklamaktadırlar. Bireyler ise finansal bilgilerinin yanında, tercihlerini, gezdikleri yerleri, kişisel fotoğraflarını cep telefonu, kişisel bilgisayar veya internet (bulut) gibi yerlerde saklamaktadırlar. Devletler ve devlet adamları bu şekliyle başta diğer ülkelerin istihbaratı olmak üzere birçok kötü niyetli devlet, kurum, terör örgütleri veya kişinin; şirketler rakipleri, devletlerin istihbarat birimlerinin, ticari fayda veya şöhret peşinde koşan siber korsanların hedefi haline gelebilmektedir. Bireyler ise genelde kişisel bilgilerini legal veya illegal yollardan ele geçirmeye çalışan şirketler, korsanlar veya devletler tarafından hedef haline gelebilmektedirler. Siber güvenliği ihlal edecek tehditler web sitelerin sizin bilgilerinizi toplaması, cihazlara bulaşan tehlikeli yazılımlar, hedefli saldırılar, kritik sistemlere sızma, hizmeti kesintiye uğratma ve benzeri şekillerde ortaya çıkabilmektedir.

Son yıllarda istihbaratın ötesinde devletlerarası savaşların da siber uzaya taşındığı, devletlerin bu düzlemi bir savaş aracı olarak kullanmaya başladığı, buna yönelik siber ordular kurdukları, bu orduları kullanarak hem istihbarat hem de kriz dönemlerinde siber saldırılar ile hizmeti durdurma saldırıları yaptıkları görülmektedir. Bu saldırılar ülkelerin nükleer tesisleri[1], enerji tesisleri[2] veya finans sektörü[3] gibi alanlara yapılabilmektedir. Bunun yanında başta haberleşme altyapısı olmak üzere teknoloji altyapısının, asgaride güvenlik sistemlerinin millileşmesi de önem arz etmektedir. Birçok teknolojik ürün üretildiği ülkenin güvenliğini öncelemesi ve bu ülkelerin istihbaratlarıyla bilinen veya bilinmeyen işbirlikleri yapmaları bilinen ve aslında beklenen bir durumdur[4]. Bağımsızlık ve dünyada söz sahibi olmak isteyen ülkelerin bu risklerin farkında olup bunları yönetiyor olması unutulmaması gereken bir olgudur. Günümüzde internetin yaygınlaşması ve hayatın bir parçası haline gelmesiyle beraber artık ülkeler arası sınırların internet üzerinden kalktığı bir dünyadayız. Ülkeler eskiden yollar üzerinden sınır kapıları ile birbirlerine bağlı iken artık fiber kablolar ile birbirlerine bağlı hale geldiler. Bu gelişmeler, iletişim, ekonomi gibi birçok alanda kolaylıklar sağlarken bağımlılıkları da arttırır hale getirmiştir.

Savaş öncesinde veyahut kriz döneminde stratejik seviyede yapılacak siber saldırılar ile düşmanın savaşma azmi ve kararlığının kırılabileceği öngörülmektedir. Hatta barış döneminden itibaren düşmanın imkân ve kabiliyetlerini geliştirecek yeteneklerine yapılacak siber saldırılar ile tehdidin daha oluşmadan yok edilmesi mümkün olabilecektir. [5]

İnternet artık hayatımızın ayrılmaz birer parçası haline gelmiştir. İnsanlar kişisel verilerini, maillerini, kontaklarını, fotoğraflarını, dosyalarını internetten kullanmaya, saklamaya başlamışlardır.

---

[1] https://en.wikipedia.org/wiki/Stuxnet 14.10.2016
[2] https://en.wikipedia.org/wiki/Shamoon 14.10.2016
[3] http://www.internethaber.com/turk-finans-sistemine-siber-saldiri-1497463h.htm 14.10.2016
[4] http://www2.tbmm.gov.tr/d23/7/7-14978s.pdf 14.10.2016
[5] Bayraktar, Gökhan; Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat

Birçok kişi günlük hayatta hava durumunu, trafik bilgisini, bankacılık işlemlerini ve bunlara benzer birçok işini internet üzerinden yapmaktadırlar.

Kurumlar ise interneti ticaretlerini geliştirmek, ürünlerine hammadde almak, ürünlerini satmak, gibi üreticiye ve tüketiciye doğrudan ve hızlı bir şekilde erişebilmek için kullanmaktadırlar. Hatta tüm yapısı internetten ticaret yapmak üzere kurulmuş şirketler dahi mevcuttur. Yakın gelecekte bir çok kurumun işlerinin neredeyse tamamını internet üzerinden yapıp takip edeceği aşikardır. Bu da aslında ticari sır kapsamında olduğunu varsaydığımız bir çok kritik verinin internette olmasını, bazı verileri bir ülkede iken başka verilerinin başka ülkede olduğu, global kompleksliğe sahip mimariler ortaya çıkabilecektir. Yani bir kurumun muhasebe sistemi bir ülkede, müşteri ilişkileri (CRM) verileri başka bir ülkede olabilecektir.

İnternetin yaygınlaşmasıyla beraber ülkemizi bekleyen olası siber tehditlere bakarsak: Bir ülkeyle olan ilişkilerde yaşanabilecek gerilim veya kopma o ülkeden alınan bulut servislerinin yavaşlatılması veya durdurulması ile sonuçlanabilir. Bu da o ülkeden servis alan birey veya kurumlarının işlerinin aksamasına, hatta durmasına neden olabilecektir.[6] Bir e-ticaret firmasının bütün işinin durmasına, satış ve sevkiyat yapamaz hale gelmesine neden olabilecektir. CRM servisi alan bir firmanın müşteri ile olan bağının kopması ve satışlarının kısa vadede azalması orta uzun vadede durması gibi durumlarla sonuçlanabilir. Biletleme, checkin gibi uçuş operasyonlarını internet üzerinden bir başka ülkeden sağlayan bir havayolu şirketi için bilet satamamak, uçaklara yolcu alamama gibi sonuçlarla sadece havayolunu değil, tüm ülke ulaşımını kaotik bir noktaya sokabilecektir. Özellikle kurumlar açısından bu tarz sistemleri planlarken sadece kısa vadeli değil uzun vadeli riskleri de öngörerek davranmaları kaçınılmaz bir zorunluluktur.

Birçok kurumun ve neredeyse tüm bireylerin buluttan kullandığı mail, dosya paylaşımı gibi servislerin kapatılması durumunda, kurumların en önemli iletişim araçlarından birinin çalışmaması sonucu kaybedecekleri ticaret potansiyeli oldukça yüksek olacaktır. Bunun devamlılık arz etmesi durumunda hem kurumlar hem de bireyler hafızalarını kaybetmiş olacaktır.

Herkesin trafikte kullandığı navigasyon sistemleri mevcut, bu sistemler kendisini kullanan kullanıcıların verilerini toplayarak anlamlı trafik verileri üretmektedirler. Bu verilere dayanaraktan kullanıcılarına en optimum rotayı önermektedir. Bu sistemler kişilerin konum bilgilerine sahip büyük verileri sürekli işlemektedirler. Tabii ki bu büyük veri istihbari manada da kullanabilecektir. Kim kiminle hangi sıklıkta görüşmekte, kim evine işine giderken hangi rotaları kullanmaktadır gibi veriler çok kolay elde edilebilecektir. Ya da bütün veriler manipüle edilerek, kasten, bir şehirde ki trafik yanlış yönlendirmeler ile daha karmaşık hale getirilebilecektir.

İnternete olan bağımlılık uluslararası arası ilişkilerde stratejik bir silaha dönüşebilecektir.[7] Önümüzdeki yıllarda bu teknolojileri elinde tutan ülkelerin diğerlerine karşı hem ekonomik hem de stratejik olarak üstünlükleri olacağı kaçınılmazdır.

Kritik altyapıların ve kamu servislerinin sürdürülebilirliği açısından internet kullanımının kurallara bağlanması ve özellikle ülke dışındaki internet servislerine olan bağımlılığının ve entegrasyonunun kontrol altında olması gerekmektedir. Kritik altyapılar ve kamu servisleri için bağımsız ve sınırları kontrol edilen yerli internet servisleri oluşturulmalıdır. Burada kalite, inovasyon ve tecrübe oluşumunu teşvik etmek adına bunun tek bir kurum tarafından oluşturulması yerine özel sektöründe dahil olduğu bir ortak bir oluşumun tercih edilmesi daha doğru olacaktır. Böylelikle özel sektör

[6] http://www.hurriyet.com.tr/google-drive-dropbox-onedrive-github-ve-archive-org-turkiyede-engellendi-40244298 14.10.2016

[7] http://www.iar-gwu.org/node/65 08.10.2016

burada oluşturacağı tecrübeyi hem yerel hem de uluslararası pazarlarda değerlendirebilecektir. Devletin burada işletici olmaktansa kural koyan ve denetleyen rolde olması tercih edilmelidir.

Bireylerin internet kullanımının doğuracağı yan etkiler özellikle Kişisel Verilerin Korunması Kanunu ile regüle edilmeye başlanmıştır. Fakat bunun sadece ülke sınırları ile kısıtlı olduğunu ve uluslararası internet servislerinin regüle edilmesinin çok zor olacağı unutulmamalıdır. Bunun için uluslararası regülasyonların hayata geçmesi için ülke nezdinde girişimlerde bulunulması gereklidir. Bireylerinde kendi verilerinin gizliliğine sahip çıkması için bilinçlendirici faaliyet ve eğitimlerin okullardan televizyonlara her seviyede yapılması bütünleyici ve etkin bir çalışma olacaktır.

Türkiye'de siber güvenlik

Türkiye'de 20/10/2012 tarih, 28447 sayılı Resmi Gazetede yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlamak ve koordinasyonunu sağlamak görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir.[8] Bu kapsamda oluşturulan Siber Güvenlik Kurulu 2013 yılında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı, 2016 yılında 2016-2019 Ulusal Siber Güvenlik Stratejisi'ni yayınlamıştır. Siber tehdit ilk defa 2010 yılında Milli Güvenlik Kurulunun gündemine girerek ülke açısından bir tehdit olarak tanımlanmıştır.[9]

Bu kurul vizyonunu "Toplumun refahı ve güvenliği ile ülke ekonomisinin büyümesine ve verimliliğine katkı sağlamak üzere bilgi ve iletişim teknolojilerinden en etkin şekilde faydalanılabilmesi için, siber güvenlikle ilgili tüm paydaşların işbirliği içinde siber uzaydaki riskleri yetkin bir biçimde yönettikleri, siber güvenlik alanında uluslararası rekabet gücüne sahip bir ekosistemin oluşmasıdır" şeklinde tanımlamıştır.[10]

Türkiye siyasi gündemin yoğun olduğu Gezi Parkı olayları[11], Rusya krizi[12], 15 Temmuz darbe girişimi sonrası[13] gibi dönemlerde yoğun siber saldırılara maruz kalmış ve bunların bir kısmı kısa süreli başarılı olmuştur.

Kritik altyapılar:

İşlediği bilgi veya verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılara kritik altyapılar olarak tanımlanmıştır. Türkiye'de bu kapsamda, 20.06.2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca, kritik altyapı sektörleri,

[8] http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf 08.10.16
[9] http://www.sabah.com.tr/gundem/2010/10/28/kirmizi_kitapa_mgkdan_vize 11.10.16
[10] http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf 08.10.16
[11] http://www.ntv.com.tr/turkiye/icisleri-bakanligina-siber-saldiri,obtLd5pnTUa1vietDFrJYA 14.10.2016
[12] http://turk-internet.com/portal/yazigoster.php?yaziid=51709 14.10.2016
[13] http://aa.com.tr/tr/15-temmuz-darbe-girisimi/darbe-girisiminin-ikinci-ayagi-siber-saldirilar-olabilir/622063 14.10.2016

Elektronik Haberleşme, Enerji, Su Yönetimi, Kritik Kamu Hizmetleri, Ulaştırma ve Bankacılık ve Finans olarak belirlenmiştir.[14]

Dünya'da siber güvenlik

AB (Avrupa Birliği), OECD (Ekonomik İşbirliği ve Kalkınma Teşkilatı), NATO (Kuzey Atlantik İttifakı) gibi uluslararası kuruluşlarla beraber tüm gelişmiş ülkelerin gündemine Siber Güvenlik konusu, özellikle 2008 yılından itibaren, girmiştir.[15]

Siber güvenlik uluslararası ilişiklerde önemli bir rol oynamaktadır. Fransa, Almanya, Norveç gibi bir çok ülke siber ajanların hedefi haline gelmişlerdir. Fransız uçakları bir zararlı yazılım nedeniyle uçuşlarına ara vermek zorunda kalmışlardır. İngiltere'de siber korsanlar savunma bakanlığının gizli ağlarına erişim sağlamışlardır. [16]

Rus korsanlar, sessiz ve yakalanmadan operasyon yapabilen, dünyanın en iyi korsanları olarak bilinmekteler. Rusya dünyadaki bilinen birçok siber olaylarla en azından dolaylı olarak ilişkilendirilmiştir.[17] Bunların en meşhuru Estonya hükümetinin Sovyet döneminden kalan bir heykeli kaldırmak istemesi sonrası üç hafta süreyle hükümet siteleri, bankalar ve üniversitelerin saldırıya maruz kalması idi. (GWU) Estonya Dışişleri Bakanı bu saldırılardan Kremlin'i sorumlu tutmuş ve daha sonra bir panel esnasında bir rus yetkili bir yönetici asistanının bunu şahsi olarak organize ettiğini ifade etmiştir.[18] Rusların yanında Amerika, Çin ve İsrail'in de siber savaş için ordular kurdukları bilinmektedir.[19]

Çinliler de 1999 yılından beri birçok Amerikan ordu, savunma ve ticari kurumlarına sızarak istihbarat çalışmaları yapmaktadırlar. Bunun yanında Çinlilerin birçok İngiliz, Alman, Japon, Hint ve Güney Kore devlet kaynaklarına sızdıklarına inanılmaktadır. Bunun yanında Çin yetkilileri Tayvan ve Amerikalar tarafından kendi sistemlerinden bilgi çalındığı iddiaları vardır. 2013 yılında Edward Snowden Wikileaks belgelerinde bunu doğrulamıştır.[20]

Dünyada ilk ve en ciddi siber savaş olarak kabul edilen Stuxnet'i ise Amerikan istihbaratının yaptığı herkes tarafından kabul edilmektedir. 2010 yılında keşfedilen Stuxnet sadece SCADA sistemlerini hedefleyen ve İran'ın nükleer programını başarısızlığa sürükleyen sıradışı ve kompleks bir sabotajdır.[21]

2013 yılında Edward Snowden tarafından ifşa edilen Amerikan Ulusal Güvenlik Ajansının (National Security Agency – NSA) büyük veri toplama programı[22] ülkelerin ne kadar kuvvetli olsalar da diğer ülkeler tarafından izlendiği ve eğer internete bağlıysanız hiçbir zaman tam anlamıyla güvende olmayacağınızı göstermektedir.

---

[14] http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf 08.10.16
[15] http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf 08.10.16
[16] Geers, Kenneth; Pandemonium: Nation States, National Security, and the Internet
[17] Geers, Kenneth; Pandemonium: Nation States, National Security, and the Internet
[18] https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia 11.10.16
[19] Geers, Kenneth; Pandemonium: Nation States, National Security, and the Internet
[20] Geers, Kenneth; Pandemonium: Nation States, National Security, and the Internet
[21] Blumbergs, Bernhards, Technical Analysis Of Advanced Threat Tactics Targeting Critical Information Infrastructure
[22] Blumbergs, Bernhards, Technical Analysis Of Advanced Threat Tactics Targeting Critical Information Infrastructure

Muhtemelen İran tarafından desteklenen Shamoon virüsü ise Suudi Arabistan'ın ulusal petrol şirketi Aramco'nun bilgisayarlarının dörtte üçündeki tüm dosyaları silmiş ve Aramco'nun sistemlerinin haftalarca çalışmasını engellemişlerdir[23]

İranlılar tarafından desteklenen Iraklı askerler, 2009 yılında Amerikan Predator, insansız hava araçlarının video görüntülerini, internetten 25,95 $'a satın alınabilecek, herkese açık bir yazılım ile takip etmeyi başarmışlardır.[24]

Suriye Elektronik Ordusu (Syrian Electronic Army – SEA) birçok eylemde bulunmuş, bunların en meşhuru ele geçirdikleri Associated Press (AP) Twitter hesabından Beyaz Saray'ın bombalandığını ve Başkan Obama'nın yaralı olduğunu duyurmalarından sonra borsaların 200 milyon dolar değer kaybetmesi olmuştur. SEA, Viber, Tango, Truecaller gibi dünyanın yaygın haberleşme uygulamalarına sızarak milyonlarca insanın haberleşmelerini takip edebileceklerini göstermişlerdir.[25]

Yukarıdaki örneklerde görülebileceği gibi siber güvenlik ile ilgili tehditler her geçen gün evrilerek daha karmaşık hale geliyor. Devletler bu tehditleri istihbarat elde etmek, diğer devletler üzerinde etkilerini arttırmak ve onları yıldırmak için yoğun bir şekilde kullanıyor. Siber güvenliğin sadece teknik bir konu olmadığı istihbarat birimleri, askeri birlikler gibi ülkenin gücünü ortaya koyan unsurlardan biri olarak uluslararası ilişkilerde önemli bir unsur haline geldiği görülmektedir. Son yıllarda Türkiye'de artan farkındalığın ve alınan aksiyonların artarak devam etmesi kaçınılmazdır.

Özellikle internetin hızlanması ve internet ekonomisinin globalleşmesi ile beraber barış dönemlerinde bir kolaylık olarak görülen bir internet hizmetinin bir kriz veya savaş anında ne kadar güçlü bir silah haline gelebileceği de göz ardı edilmemeli. Bu kapsamda kritik altyapı kavramı gerekirse özel sektörü de kapsayacak şekilde yeniden tanımlanarak ülkenin her koşulda kendi sınırları içerisinde yaşayabilir, üretebilir olması sağlanmalıdır.

Güvenlik altyapılarının millileştirilmesi, yetişmiş eleman sayısının arttırılması, siber istihbaratın güçlendirilmesi Türkiye'nin yakın gelecekte uluslararası arenada daha etkin durmasını sağlayacaktır.

[23] Geers, Kenneth; Pandemonium: Nation States, National Security, and the Internet
[24] http://www.wsj.com/articles/SB126102247889095011 11.10.16
[25] Geers, Kenneth; Pandemonium: Nation States, National Security, and the Internet