DÖRDÜNCÜ SANAYİ DEVRİMİNİN BİR SONUCU OLARAK SİBER TEHDİTLER VE SİBER GÜVENLİĞİN AİLE, ŞİRKET VE DEVLET BAZINDA ÖNEMİ[1]

Belma KUVANCI
Ankara Hacı Bayram Veli Üniversitesi
Yüksel Lisans Öğrencisi

Doç. Dr. Fetullah AKIN
Ankara Hacı Bayram Veli Üniversitesi
İktisadi ve İdari Bilimler Fakültesi

ÖZET

İnsanlık tarihinde eşi benzeri görülmemiş bir hız ve derinliğe sahip aynı zamanda yayılma ve genişleme bakımından da tüm dünyayı saran dördüncü sanayi devrimi etkilerini göstermeye devam ediyor. Dördüncü sanayi devrimi dediğimiz ve Endüstri 4.0 da denilen bu döneme 2000 yıllarında geçilmeye başlanmıştır. Günlük yaşamda işlerimizi kolaylaştıran yeni teknolojiler ile eskiden olduğundan çok daha kolay ve hızlı işlerimizi yapabiliyoruz. Şirketler de keza verimliliklerini kat kat arttırmış durumdalar. Devlet bazında da işler kontrol altında olduğu görülmektedir. Vatandaşlık işleri, asayiş, diplomasi, askeri çalışmalar ve ekonominin kayıt altında tutulması gibi işler rahatlıkla yürümektedir. Ancak kullandığımız bilgisayar donanımları, akıllı telefon ve akıllı cihazlar, yapay zekâ olarak kullanılan sistemler, internet alt yapıları, siber uzaydaki sistemler, yazılımlar gibi pek çok teknolojik çıktı başkaları tarafından izlenip, kopyalanıp, çalışması engellenip, ya da istemsiz çalışması sağlanıp vs. bize sorun olarak geri dönebilir. Ailenin fertleri olarak; önce teknolojiyi öğrenip, tanıyıp, teknoloji ile barışmamız gerekmekte; sonra da yeni jenerasyona sorumluluk bilinci ve siber güvenliğin önemini aşılayarak vatandaş olarak tedbir almak zorundayız. Ardından şirketlerin ve devletlerin görev ve sorumlulukları başlamaktadır. İçinde bulunduğumuz ve sonunu öngöremediğimiz bu dönemi zarar görmeden yaşamanın ve bir sonraki döneme hazırlanmanın tek yolu, teknolojiyi üreten ve ihraç eden olmaktan geçmektedir.

Anahtar kelimeler: Endüstri 4.0, Dördüncü Sanayi Devrimi, Siber, Siber Tehdit, Siber Güvenlik, İnternet, Zararlı Yazılım

1 Bu makale; "Dördüncü Sanayi Devriminin İstihdama Olumsuz Etkilerinin Değerlendirilmesi ve Geleceğin Olası İstihdam Fırsatları" isimli Yüksek Lisans Tezinden Türetilmiştir.

IMPORTANCE OF CYBER SECURITY ON THE BASIS OF FAMILIES, COMPANIES AND GOVERNMENT AS A CONSEQUENCE OF FOURTH INDUSTRIAL REVOLUTION

ABSTRACT

The fourth industrial revolution continues demonstrating its effects having unprecedented speed and depth ever seen in human history and extending all over the world in terms of its expansion. Transition to this period we call the Fourth Industrial Revolution, which is also referred to as Industry 4.0, got under way in the 2000's. We are able to do our works much more easily and faster thanks to the new technologies facilitating our works in the daily life. Accordingly, companies have increased their profitability by several times. Works are now under control for the government as well. Works such as citizenship affairs, public order, diplomacy, military works and keeping economy under record go on comfortably. However, many technological outputs such as computer hardware, smart telephones and smart devices, systems operated by artificial intelligence, internet platforms, systems on the cyber space and software extensively used by us may eventually prove problematic for us as they might be tracked and copied by others preventing their operation or ensuring their undesired operation, etc. As the members of a family, we must first learn about technology, getting us in good terms with it and then, take the initial measure as a citizen by impressing awareness of responsibility and importance of cyber security on the next generation. This is followed by the tasks and responsibilities of companies and governments. Being a producer and exporter of technology is the only way to live this period we are currently going through without any damages being unable to predict its end so that we can prepare for the next period.

Keywords: Industry 4.0, Fourth Industrial Revolution, Cyber, Cyber Threats, Cyber Security, Internet, Malicious Software

GİRİŞ

Birey olarak hayatımızdaki her anı paylaşarak nasıl daha güvenli yaşayabiliriz? Şirket olarak verilerimizi birkaç harf, rakam ve şekilden ibaret şifrelere emanet etmekle şirketimizi koruyabilir miyiz? Devlet olarak internet başta olmak üzere kullandığımız teknolojileri başka devletlerden ithal ederek vatanımızın bütünlüğünü ve milletimizin bağımsızlığını tavizler vermeden nereye kadar sürdürebiliriz? Bir bütün olarak baktığımızda dünya, bir yandan daha

iki yaşında elinde bir tabletle ya da telefonla internette oyun oynayan çocuklar yetiştirirken, diğer yandan da iki yudum su için yalınayak nehirler geçmek zorunda olan çocukları yaşarken, nasıl barış ve huzurun korunduğu ve tesis edildiği bir yer olacak? Evimizden, işimizden, vatanımızdan ve yeryüzünden gidecek başka bir yer var mı? Eğer yok ise, ki başka yer yoktur, bu dünyada insanoğlu elimizdekileri bozmadan koruyarak yaşamak zorundadır.

Bu çalışma, dördüncü sanayi devriminin getirdikleri ve götürdükleri üzerine araştırmamız sürecinde ve bu devrimin yumuşak karnı diyebileceğimiz siber güvenliğin, sandığımızdan çok daha hayati öneme sahip olduğunun farkındalığı ve bu farkındalığı topluma da anlatma arzusundan doğmuştur.

Araştırma konusunu seçerken, araştırma evrenini dördüncü sanayi devriminin getirdikleri olarak belirlendi, örneklemi ise, internet teknolojisi üzerine seçildi. Daha da sınırlandırabilmek adına siber güvenliğin ne olduğu, nasıl sağlanabileceği, sağlanmadığında neler olabileceği hakkında teknik bilgiden ziyade sosyal içerikli farkındalık, uyarı ve tedbir önerilerine ağırlık verildi.

Türkiye'de yaklaşık 2016'lara kadar konu hakkında Türkçe yayın kısıtlı iken son 3 yılda katlanarak artmıştır. Bunun sebebi siber alanlar ile ilgili ihtiyacın artmasıdır. Dolayısıyla yeni yeni tehlikelerini algılamaya başladığımız internet dünyası, gerekli tedbirler artmazsa içine düştüğümüz kör kuyudan farksız bir durumda olabiliriz.

Fiziki mekânlarda, gerçek kişilerle gerçek araçlarla yapılan işler, fiiller, eğlenceler, alışverişler, görüşmeler, oyunlar, arkadaşlıklar, aktivist eylemler ve akla gelen pek çok şey artık dijital makinelerin, yazılımların, her türlü teçhizat ve donanımın, internetin, yapay zekânın, sosyal medyanın gücüyle ve mekân, sınır, zaman mefhumu olmadan yapılabilir haldedir. Bunlar bu kadar kolay olurken aynı şekilde korunması da bir o kadar zor olmaktadır. Artık suç, güvenlik, tehdit, saldırı, savaş, korunma, istihbarat, gibi terimlerin tanımları da evrim geçirmiştir. Sanal dünyanın tehdit ettiği gerçek dünyada kendimizi tüm bunlardan izole edebilmemiz mümkün değildir.

Makalenin yazılma amacı okuyucuyu biraz korkutmaktır; korkutmaktan kasıt, tehlikenin farkına vardırmaktır. Ancak korkmak yetmez, işe de yaramaz. Artık bulunduğumuz teknolojik seviyeden geri de gidemeyiz. Bunu kontrol etmeli, hatta başarabiliyorsak avantaja çevirmeliyiz. Bu nasıl başarılır diye düşünürken; ülkemizdeki artan eğitimli işsizler ordusunu neden ülkemizin eğitimli siber ordusuna dönüştürmüyoruz sorusu aklımıza geldi; neden olmasın?

İçinde yaşadığımız çağ geri durulacak değil üzerine gidilecek bir çağdır. Sun Tzu "savaş yeteneği olanların düşman ordusunu savaşmadan bastıranlar

olduğunu *söylemiştir; ş*ehirleri saldırmadan ele geçirebileceklerini ve devletleri operasyon yapmadan devirebileceklerini" eklemiştir. Teknolojiyi yönetebilenler günümüzün savaş yeteneği olanlarıdır. Sun Tzu'nun yüzyıllar önce kastettiği bu olmasa da günümüzde aynı mantığı siber mücadeleler için düşünebiliriz.

Günümüzdeki siber savaş sadece bilgisayarlar üzerinde değil siber uzaydaki tüm teçhizat ve sistemlere karşı da sürdürülmektedir. O sebeple büyük resme bakmalı ve olayın sosyal medya hesaplarımızın ele geçirilmesinden çok daha vahim olduğunu idrak etmeliyiz.

İçinde yaşadığımız dönemin özellikleri anlatılarak konuya başlandı. Yaşadığımız döneme geliş sürecimiz devrim niteliğindeki değişmelere değinilerek anlatıldı. Bu değişmeler avcılık ve toplayıcılıktan tarıma geçişin ipuçlarına değinilerek, birinci, ikinci, üçüncü ve dördüncü sanayi devrimlerine geçişlerin tarihi ve parametreleri verilmeye çalışıldı. Çağımızın vebası olarak ortaya çıkan zararlı yazılımlar ve siber suçların vardığı ve varabileceği boyutlar irdelendi. Bunlara karşı önlemlerin alınmasının gereği ortaya konuldu.

1.TARİHSEL SÜREÇ

Nasıl Bir Dönemde Yaşıyoruz?

Çocuklarımız bu dönemin içinde doğdular; özellikle 2000 sonrası doğanlar yani Z kuşağı da denilen bu kuşak teknolojinin, siber dünyanın, dördüncü sanayi devriminin tam ortasında doğdu. Dolayısıyla bu çocuklara değişik isimler verdiler, örneğin dijital yerliler terimi kullanıldı (Turhan ve Okcu, 2018: 149). Bu terim ilk kez 2001 yılında eğitim danışmanı olan Marc Prensky tarafından kullanılmıştır. Prensky 1990'dan sonra doğanları tümüyle bu tanım içerisinde değerlendirmiştir. Bu değerlendirmenin dayanağı doğduğu anda dijital varlıklarla tanışmış ve dijital dünyanın içine doğmuş olmalarıdır. 1990 öncesi doğanlar dijital ile hayatlarının belli bir döneminde tanışmış oldukları için bu kimselere de dijital göçmenler demeyi uygun bulmuştur (Turhan ve Okcu, 2018: 150).

Her ne kadar çocuklarımız bu dünyanın içine doğsalar da onlar da biz de bu dönemi sindirerek yaşayamıyoruz. Dışarıdan bahçemize ithal edilmiş yeni bir ev gibi kapalı kutu misali bir anda kendimizi içinde bulduğumuz yeni bir dünya ile karşı karşıyayız. İçerisinde nasıl tehlikeler var, yaşadıkça gördüğümüz çoğu zaman bunu bile göremediğimiz, fark ettiğimizde de ne yapacağımızı bilemediğimiz yeni bir dünya... Bu dünyanın suçları da gerçek dünya gibi doğrudan zarar verici olmuyor bazen, gizliden derinden oluyor. Gerçekten, biri evinize girip cüzdanınızı ve içinden paranızı alsa, kimliğinizi masanın üzerinden

biri alıp yok etse, şirketinizden bir dosya kaybolsa, bir kitabınız bir makaleniz bir raporunuz çalınsa, devlet arşivlerine biri sızarak oradaki vatandaşların ve devletin dosyalarını çalsa, askeri bir haritayı, bir savaş planını, üretilecek bir teçhizatın projesini biri çalsa fark edersiniz. Ancak, yenidünyada siber olarak yapılan işleri bu açıklıkta fark etmek bazen mümkün olmamakta, bazen de fark etmek çok zor olmaktadır.

Şu anda bile bu makaleyi yazarken kullandığımız bilgisayara birileri göz atıyor olabilir; ya da siz bu makaleyi okurken birileri de sizin bilgilerinizi okuyor olabilir; ancak hiçbirimiz bunun farkına varamıyoruz (Falkner, 2012: 13).

Yenidünyada bilgi artık fiziksel olarak kâğıtlara, kitaplara yazılıp basılmış değil, dijital ortamlara aktarıldığından çalma olayının adı kopyalama, hırsızlığın adı da siber suç olarak değişmiştir. Siz bilgisayarınızı açtığınızda dosyanız kopyalanmış (çalınmış) olsa dahi yerinde durduğundan bunu hemen fark edemeyeceksiniz. Başınıza kopyalanmış ya da siber suç olarak alınmış bilgiler yüzünden bir iş geldiğinde belki aklınıza gelecek. Benzer şekilde, bir askeri operasyonu yönetirken karşı tarafın buna göre tedbirini çoktan almış olduğunu gördüğünüzde, bir ihaleye girdiğinizde şirket olarak rakibinizin hatta rakibiniz bile olmayan bir şirketin sizin projenizin ve tekliflerinizin aynısını masaya koyduğunu gördüğünüzde fark edeceksiniz ama bu fikri ben bulmuştum demeniz işe yaramayacak, ihaleyi ya da savaşı kaybettiğinizde iş işten geçmiş olacaktır. Bu şekilde başınıza gelmesi muhtemel bu en kötü vakalarla karşılaşmadan önce bunu tahmin edemediğiniz için ve önlem alamadığınız için, o gün geldiğinde çok konuşulan siber suçlara karşı siber güvenlik önlemlerini niye yükseltmediğinize belki ömür boyu pişman olacaksınız.

Daha basit örnekler de verebiliriz: köyünde, evinde oturup birkaç komşuyla sohbetten başka bir dünyası olmayan bir ev hanımını düşünelim. Bu konularla hiç alakası yokmuş gibi duruyor. Ancak evine alacağı bir telefon, ya da bir akıllı ev aleti ile başına olmadık işler gelebilir. Çocuğunun sosyal medyada evin hangi köşesini paylaştığını takip edemiyorsa, konum bilgilerinden kimlik bilgilerine kadar, aldıkları yeni ürünlerden belki de mahrem fotoğraflara kadar denetleyemiyorsa tehdit altındadır. Örneğin evden dışarı çıkarken belli bir örtünme ölçüsü olan muhafazakâr bir kadının ev içerisindeki daha rahat bir halinin, tüm internet mecralarında dolaşmasını nasıl karşılayacağını tahmin edelim. Kapının önüne çıkmadığı halini artık tanıdık tanımadık herkes görmüş oldu ve geri alma şansı hiç yok. O kadın için bu bir yıkım sebebidir. Mahremiyetimizi korumak da can ve mal güvenliğimizi korumak kadar önemlidir. Hepsi için topyekûn farkındalık ve topyekûn mücadele gereklidir.

Bu noktaya nasıl geldik?

İnsanlık tarihi gelişmelerle, devrimlerle, buluşlarla ve ilerleme için sürekli olarak çalışmalarla doludur. Avcılık ve toplayıcılıktan tarıma geçiş ilk büyük değişimdir, yaklaşık 10 bin yıl önce bu değişim gerçekleşmiştir. Bu değişim sürecinde hayvanların da ehlileştirilmesi sağlandı, hayvan gücü sayesinde daha fazla ve verimli tarım yapmak mümkün hale geldi, böylece köyler ve kentler oluşmaya başladı.

Tarım devrimi 18. Yüzyıla kadar sürdü. 18. Yüzyılın ikinci yarısında Endüstri 1.0 denilen birinci sanayi devrimi başladı. Tarihlendirildiğinde, yaklaşık olarak 1760'lardan 1840'lara kadar süreç devam etti, sürecin karakteristiğini ortaya koyan olgular ise demiryollarının inşası ve buhar makinesinin üretime sokulmasıyla mekanik üretimin başlanılmış olmasıdır.

1840'lardan 1960'lara kadar süren Elektrik ve montaj hattının bulunmasıyla seri üretim hız kazandı; içten yanmalı motorların gelişimi de önemli ölçüde bu dönemin kazanımlarıdır; böylece bu döneme Endüstri 2.0 denilen ikinci sanayi devrimi denildi.

Endüstri 3.0 denilen üçüncü sanayi devrimi ise 1960'lardan 2000'lere kadar süren anabilgisayarlar ve sonrasında kişisel bilgisayarların öncülük ettiği internetin bulunduğu bilgisayar devrimi ya da dijital devrim de denilen bir dönemdir. Aslında bilgisayar ve internet temelli teknolojiler kullanılmaya devem etmekle beraber çok fazla evrim geçirmiştir.

Endüstri 4.0 denilen içinde bulunduğumuz dördüncü sanayi devrimi bilgisayarların çok hızlandığı, internetin yaygınlaştığı, yapay zekanın bulunduğu, nesnelerin interneti kullanılmaya başlandığı, akıllı cihazların, giyilebilir teknolojilerin, akıllı arabaların, akıllı şehirlerin, yapay zekayla donatılmış robotların, genetikte insan genomu çalışmalarının, 3D baskının, siber uzayın, dronların, İHA'ların, özellikli malzemelerin bulunarak hızla yaygınlaştığı bir dönem olarak tarihe geçmektedir (Schwab, 2018: 16).

Şu an dünyamızda bilinen pek çok parametre en fazla 300 yıllık bir tarihe sahiptir. Fakat insanlık tarihinde çok çok kısa sayılabilecek 300 yıl, paradigma değişimlerine sebep olmuştur. Enerji devrimi ile iş yeri tarladan çok farklı bir mekân olan fabrikalara dönüşmüş, işte geçirilen süre de düzenli ve belirlenmiş saatlerle tanımlanmıştır. Fabrika işçisi olmayan diğer bireylerin, aile ve sosyal çevrenin o iş mekânıyla ve iş zamanıyla ilgisinin olmadığı bunların tamamen ayrıştırıldığı bir düzene geçilmiştir. Bugünün rutinleri tarım toplumunda yaşayan birine söylense sanırım güler geçerdi. Dijital devrim de bunun gibidir, biz gelecekte neye evirileceğini çok kestirememekle beraber gördüğümüz ve algı-

ladığımız şey, değişikliklerden öte değişimi ölçen cetvelin değişmiş olmasıdır. Dolayısıyla yeni paradigma, yeni ölçüler, yeni evren kapımızdadır. Bize düşen hızına ayak uydurabilmektir (Canan ve Acungil, 2019: 65).

Dördüncü sanayi devriminin bu baş döndüren icatlar çağı olması ve ortaya çıkan buluşların yine hiç görülmemiş bir hızla yaygınlaşması sonucu ortaya çıkan yeni düzene ve yeni alışkanlıklara hukukun ve insan doğasının aynı hızla yetişememesi sonucu bazı tehlikeler de beraberinde hayatımıza girmektedir.

Yeni teknolojilerin yayılma hızına karşılaştırmalı bir örnek vermek gerekirse; birinci sanayi devriminin simgesi olan iplik makinesinin Avrupa'nın dışında yayılması yaklaşık 120 yıl sürmüşken, dördüncü sanayi devriminin katalizörü olan internetin tüm dünyaya yayılma hızı sadece 10 yıl hatta daha da kısa sürmüştür(Schwab, 2018: 17).

İnternetin hızla yaygınlaşması sonucu aynı hızla güvenliğinin sağlanamamasını doğurmuş ve güvenlik açığı giderek bir zafiyet konusu olmuştur. Dolayısıyla da hayatımıza korunması gereken yeni bir alan eklenmiş olup, korunma yol ve yöntemleri karmaşık fakat hayati derecede önemli hale gelmiştir.

Güvenliğin özellikle de bilgi güvenliğinin temel unsularından sayılan gizlilik, bütünlük ve erişim ilkelerinin zarar görmesi kolaylaşmış ve bunların zarar görmesini önleme ihtiyacı önem kazanmakla beraber önleyebilme ve koruyabilme ihtimalleri de zorlaşmıştır (Başaran, 2019:12). Siber tehditler bu boyutlara ilerlerken siber güvenlik günlük hayatımızın bir parçası olma yoluna gitmektedir.

2. BAZI KAVRAMLAR VE DİJİTALİ ANLAMAK

Dördüncü sanayi devriminin getirdiği yenilikler ile hayatımız kolaylaşırken bir o kadar da tehditlere açık hale gelmiştir. Bu tehditlerden korunmak için öncelikle nelerle karşı karşıya olduğumuzun anlaşılması ve baş etme yolları hakkında temel önerilere değinmek yerinde olacaktır.

İnternet

Dijital dünyayı uçsuz bucaksız yapan elbette ki internettir. İnternetin doğuşunu hatırlatmak çok pembe görünen bu dünyaya biraz daha şüpheci bakmamıza yardımcı olabilir belki.

1960'lar, ABD ve Sovyetler Birliği arasında süren soğuk savaşın en şiddetli yıllarıydı. Herkes sonunun nereye varacağını korkuyla beklerken ABD Savunma Bakanlığının bir birimi olan Advanced Research Projects Agency (ARPA)

tarafından ARPANET isimli bir ağ geliştirildi. Bu ağın amacı Pentagona proje ve veri sağlamaktı. Bu ağ gelişerek ve dönüşerek en sonunda İnternet ağına dönüşmüştür (Aust ve Amman, 2018: 16). Tüm dünyaya ihraç edilerek tüm dünyanın verileri en nihayetinde Amerika'da toplanıp işlenmeye ve bu büyük veri yığınlarından anlamlı yorumlar ve sonuçlar üretilmeye başlanmıştır. ABD askeri projesi olarak başlayan bu proje sayesinde ABD, ülkeleri, halkları, ekonomileri, orduları, siyasetçileri ve her kimi isterse takip edebilen, yön verebilen ve üzerinde istediğini yapabilen bir süper güç haline gelmiştir. Bu gelişmeler silsilesine bakarsak, siber uzayda ve bilişimde ABD ile eşitlik hatta ona karşı üstünlük sağlanamazsa, ezici, korkutucu ve totaliter bir rejimi akla getiren tek kutuplu ve tek merkezli bir yönetime hızla sürüklenen bir hayata boyun eğmek zorunda kalabiliriz.

İnternetle doğrudan alakalı yeni bir terim; nesnelerin interneti (IoT) artık telefon, tablet ya da bilgisayarlardan hariç evimizdeki buzdolabı, kombi hatta perdelere kadar pek çok nesne internete bağlanmaya başlandı. Kaldı ki kendi aralarında iletişim kurup kendilerini yönetebiliyorlar. Bu da evin en gizli yerlerine kadar bütün özel hayatımızın internet ortamına aktarılması ve güvenlik ve gizliliğin ortadan kalkması demektir(Şeker, 2018: 164). Bir zaman sonra artık nesnelerin interneti (IoT), her şeyin internetine (IoE) dönüşecek. Şimdinin bağlantıları yarının altyapısını oluşturma çabasıdır ve bu gelişim kaçınılmazdır. (Herzberg, 2017: 22). Sonunda internet ve getirdikleri sayesinde bir şeyleri kontrol ederken, internet bağlantılarının bizleri, kendimizi, ailemizi, işimizi hatta ülkemizi kontrol edip yönettiğine şahit olabiliriz.

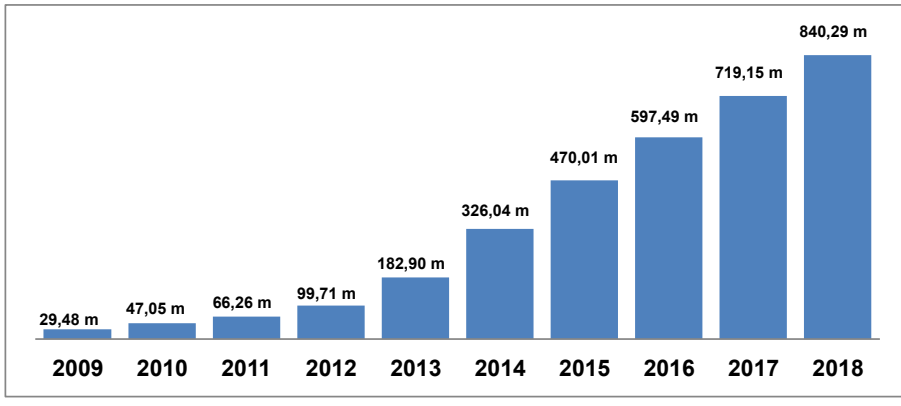
Zararlı Yazılımlar

Zararlı yazılımlar, kötü amaçlı yazılmış programlar ve kodlar olarak genellenebilir (Başaran, 2019: 15.) Zararlı yazılım kendi isteğimiz ile paylaştığımız bilgilerden ayrı bir şeydir. Aslında burada geniş çaplı bilgi verebilmek çok mümkün değil. Çünkü her gün 350.000 den fazla zararlı yazılım tespit edilmekte (Başaran, 2019:11). Burada zararlı yazılımların ilk çıkışları ve en bilinenlerinden örnekler vererek neden korunmamız gerektiğine değinilecektir. Zararlı yazılımlar virüs, solucan, truva atı, keyloggler (kaydedici), DoS, DDoS, rootkitler, botnet, gibi farklı isim, yöntem ve şekillerde olabilir. Teknik olarak tek tek incelemek başka bir teknoloji makalesinin konusu olması gerekliliği düşüncesi ile burada değinilmeyecek olup zararlı yazılımların işlevleri hakkında bilgi vermekle yetinilecektir. Zararlı yazılımlar, virüsler genellikle bir e-posta eki olarak bilgisayara bulaşır ve bilgisayarın performansını düşürme, bilgi kopyalama ve sistemi çökertme üzerine çalışırlar. Keyloggler bir yazılım ve donanımdır. Bunlarda bilgi kopyalama ve ekranı okuma özelliğine sahiptir. Truva atları da girdiği bilgisayarı uzaktan erişime açan yani içerden kapıyı

açan casus işlevi görürler. Genelde ücretsiz ve cracklenmiş (kırılmış) yazılımlar ile gelirler. Trend Labs bir araştırmasında veri hırsızlığı yapan yazılımların Truva atı kullanma oranının, 2007 yılında %52, 2008 yılında %87 ve 2009 yılında %93'lerde olduğunu açıklamıştır. Solucanlar herhangi bir dosyaya gerek kalmadan çalışırlar. Bulaştığı yerde çok hızlı ve çok sayıda çoğalarak sistemi etkisiz hale getiriler. Dos tek makineden DDoS çoklu makinelerden saldıran zombi bilgisayarları BOTNET (Robot Network) ağına dahil ederek hedef sistemi hizmet dışı bırakan zararlı yazılımlardır (Kurgan, 2017:113-124). Bu yazılımlar sebebiyle meydana gelmiş bazı çarpıcı örneklere yeri geldiğinde atıf yapılacaktır.

Zararlı yazılımların boyutunu anlamak için aşağıdaki tabloda bağımsız anti-virüs test kuruluşu AV-TEST tarafından yayınlanan rakamları bulabilirsiniz.

Grafik: 1 AV-TEST Tarafından Tespit Edilen Zararlı Yazılım Sayıları (m=milyon)



Kaynak: Başaran, A. (2019). *Zararlı Yazılımlar*, İstanbul: Arion Yayıncılık, 149

Bunların sadece yakalanabilen zararlı yazılımlar olduğunu hesaba katarsak sayının daha da büyük olmasını beklemek hayal değildir. Ayrıca siber güvenliği sağlamak noktasında en büyük mücadelenin zararlı yazılımlara karşı sürdürülmesi gerekliliğini de bu tablo ispatlamaktadır.

Siber (…)

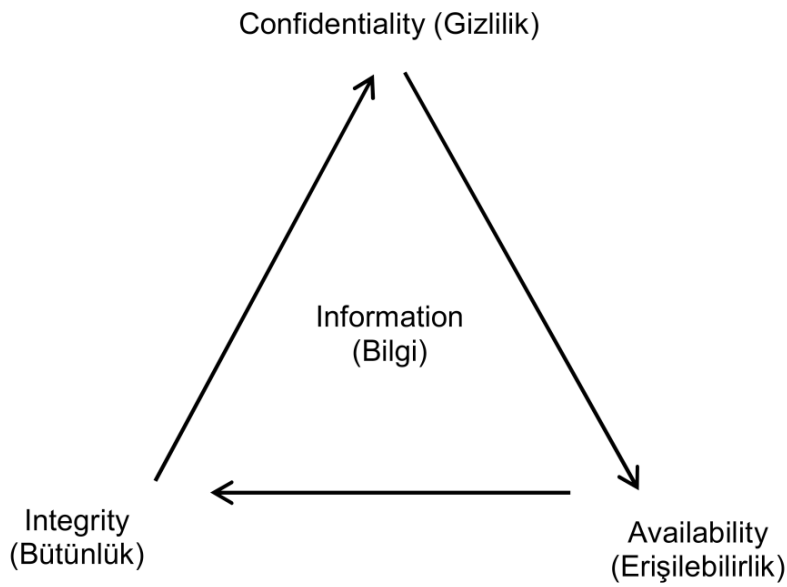
"Siber" kelimesi İngilizce "cyber" kelimesinden uyarlanmıştır. Bu da "bilgisayar ağlarına ait" demektir. Sibernetik kavramından türetilmiştir. Sibernetik modern yaşamda ilk kez 1948 yılında NorbertWeiner isimli Amerikalı bir bilim adamı tarafından "hayvanlarda ve makinelerde iletişim ve kontrol bilimi" için kullanılmıştır. Türkçede sibernetik TDK'da "güdüm bilimi" olarak tanımlanmıştır (Erdoğan, 2018: 49). Siber güvenlik denildiğinde mutabık kalınmış

bir tanım olmamasına rağmen bilgi güvenliği anlamında basitleştirebiliriz. Bilgi güvenliği kişisel ve kurumsal bilgilerin korunmasını gerektirir.

Siber uzay kavramından bahsederek devam etmek gerektiğinden doktrine başvurarak şu tanımları verebiliriz.

> *"İşlemci ve kontrolörlerin bulunduğu internet, telekomünikasyon ağları ve bilgisayar sistemlerini de içine alan, birbirine bağlı bilgi teknolojileri altyapılarının olduğu küresel bir alan"* şeklinde tanımlanmaktadır. *"Bilgi teknolojileri tarih boyunca dünya haricinde uzayda başka dünyalar arayan insanoğluna alternatif bir uzay sunmaktadır. Bu uzay, ev ve işyerlerine girecek kadar yakın, bütün evreni saracak kadar büyük, canlılara ve bilgiye parmak ucu ile dokunabilecek kadar uzaklıkta olan ve yaşantıları her şekilde etkileyebilen siber uzaydır"* denilmektedir (Yıldız, 2007: 35).

Siber güvenlik için yani siber uzayın güvenliği için bilgiye dair sayılan 3 ana güvenlik prensibinden bahsedilmişti. Bunlar aslında temel gerekliliklerdir. İlki bilginin gizliliği, ikincisi bilginin bütünlüğü sonuncusu da bilginin bütünlüğüdür (Eren, 2017: 23). Ayrıca bu gereklilikler siber güvenliğin hedefleri olarak da sayılmaktadır (Eren, 2017: 23).



Şekil: 1 Siber Güvenliğin Hedefleri
Kaynak: Eren, 2017: 23

Bir başka çalışmada siber güvenlik prensipleri arttırılarak 9 adet gereklilik şeklinde yayınlanmıştır. Bilginin korunmasının önemi açısından bu 9 prensip aşağıdaki tabloda gösterilmektedir.

Tablo: 1 Temel Güvenlik Prensipleri

No	Prensip(Tr.)	Prensip (İng.)	Kısa Açıklama
1	Gizlilik	Confidentiality	Yetkisiz erişime karşı koyma
2	Bütünlük	Integrity	Yetkisiz değişikliğe karşı koyma
3	Erişilebilirlik	Availability	Erişilmezliğe karşı koyma
4	Sahiplik	Possession	Çalınmaya veya kaybolmaya karşı koruma
5	Yararlılık	Utility	Gerektiği gibi kullanılamamaya karşı koruma
6	Gerçeklik	Authenticity	Gerçeği sağlamamaya karşı koruma
7	İnkar Edilemezlik	Non-repudiation	İnkar etmeye karşı koruma
8	Yetkili Kullanım	AuthorizedUse	Yetkisiz kullanıma karşı koruma
9	Mahremiyet	Privacy	Kişisel bilginin ifşasına karşı koruma

Kaynak: Pazoğlu ve Yücesoy; 2019: 8

Siber uzayda bilgimizi koruyamazsak ne olur? Siber suçlular siber suçlar işleyerek bizlere zarar verebilirler. Siber suç kavramı genel bir ifade olup içinde sanal suçları, bilgisayar suçlarını yani bilişim suçlarını da barındırmaktadır (Erdoğan, 2018: 52). Türkiye'de artık bilişim suçu kavramı yaygın olarak kullanılmaktadır. Bilişim suçlarını dar ve geniş anlamlarında ikiye ayırabiliriz: Dar anlamıyla, "bilişim sisteminin kendisinin ya da bilişim sistemi içerisinde bulunan verilerin hedef alındığı ve bilişim teknolojilerinin kullanılması suretiyle ya da bilişim araçlarına doğrudan fiziki müdahaleyle işlenen suçlardır" şeklinde tanımlanırken; geniş anlamıyla, "herhangi bir şekilde suçun icrasında bilişim sistem ya da araçlarının kullanıldığı ya da bilişim sistemlerinin veya içindeki verilerin hedef alındığı suçlardır"(Erdoğan, 2012: 52) şeklinde tanımlanmaktadır.

3. SİBER MÜCADELE AİLE İÇİNDE BAŞLAR

Şu anki aile yapılarına, aile içi bireylerin dijitale olan bakışlarına ve bu konudaki bilgi ve kullanım eğilimlerine göre bazı sınıflandırmalar yapmak gerekecektir. Elbette bilimsel çalışmalarda genellemeler arzu edilmez. Fakat dijitaldeki şuan ki hızlı gelişim nedeniyle kuşak farkları genellemeleri kabul ettirecek düzeyde ve keskinliktedir. Bunun için X, Y ve Z kuşağı denilen 3 ayrı kuşaktan bahsedilir (Turhan, Okçu, 2018: 140-150.) Bizim en çok korumamız gereken Z kuşağı denilen, dijital yerliler vs gibi pek çok isim takılmış olan 2000 yılı sonrası doğan milenyum çocuklarıdır. Bu tabi 1999 yılının aralık ayında doğanlar girmez diye bir kesinlikte olmamakla beraber genel tabir milenyum çocukları şeklindedir.

Y Kuşağı dediğimiz 1980 ve 2000 arası doğanlardır. Bu kuşak dijitale yetişmiş, kullanım olarak hayatına sokabilmiş, ancak kendini dijitale kaptırmamış son kuşaktır. Çünkü Z kuşağı dijital dünyanın içine doğmuşken, Y kuşağının dünyası şekillendikten sonra dijital onların dünyasına doğmuştur. Aradaki bu fark pek çok farkı da doğurmuştur. Örneğin Y kuşağı aile içi değerleri, sosyal değerleri, vatana millete karşı bağlılığın önemini, inanç değerlerini, arkadaş sohbetlerini, yardımlaşmayı, uluslararası politik sorunları, terör, açlık, doğal afetler, suçlar gibi siyasi, sosyal, ekonomik, demografik vs. pek çok sorunla mücadeleyi benimsemiş, bunlara duyarlı yetişmiş, hayataki amaçlarını bunlara göre şekillendirmiş ve günlük yaşamlarında da bunları ihmal etmemiş belki de son kuşaktır.

X Kuşağı 1980 öncesi doğmuş ve şuan yaşamın içinde Y kuşağı olan çocuğunun çırpınışları ile, Z kuşağı olan torununun vurdumduymazlıklarını anlamaya çalışırken kafası karışmış bir kuşaktır. Teknolojiye ayak uyduran istisnalar dışında genel çoğunluk günlük Facebookta vakit geçirme, internet haberleri okuma ve WhatsApptan haberleşme dışında aktif olarak teknoloji ile çok da fazla ilgilenmemekte ve geleneksel günlük rutinlerine devam etmektedir.

Aileler çocuklara teknoloji kullanma konusunda örnek olmalıdır. Teknolojiyi kullanmanın hak olduğu kadar sorumluluk olduğunu da vurgulamalı ve öğretebilmelidirler. Teknolojinin getirdiği sorumluluklar aile içerisinde beraberce tartışılmalı ve internet bilgilerinin doğruluğuna şüpheyle yaklaşılması gerektiği ve sorgulanıp sonra kullanılması gerektiği alışkanlık haline getirilmelidir. Aksi takdirde internetteki bilgi çöplüğü ve bu çöplüğün bir parçası olma hali gerçek yaşamda pek çok sıkıntı doğurabilir. İnternet ve sosyal medyanın yarattığı bir başka sorunlar silsilesi de şöyle gruplanmaktadır. İlki; tüketim odaklı kapitalist bir zihniyet ile sahip olduğu hiçbir şeyden yetinmeme hali bir kişilik bozukluğu yaratabilmektedir. İkincisi; seküler ve ahlak dışı unsurları doğal

göstererek kültürel yozlaşma yaratabilmektedir. Üçüncüsü; Psikolojik toplum mühendisliği ile irade kullanmayı özgürlükten çıkarıp fark ettirmeden ipotek altına alıp, siyasi ve ideolojik olarak yönlendirmeler yapabilmektedir. Dördüncüsü; insanların yaşam algılarını değiştirerek ev içi mahremiyeti ortadan kaldırabilmektedir. Bu da her anını paylaşma isteği, evin içinde dahil her durumunu mahremiyet gözetmeden paylaşma hedefi ve ilgileri üzerinde toplama amacı güvenlik zafiyetine giden çok tehlikeli bir kullanım şekline dönüşebilmektedir (Dağıtmaç ve Ekmen, 2019: 66-67).

Artık yeni nesli internetten koparmak mümkün değildir. Z kuşağı dediğimiz yeni neslin kullandığı cihazlara bakarsak dizüstü bilgisayar kullanımının azaldığı, yerine cep telefonu kullanımının arttığı görülmektedir. Forbes dergisinin yaptığı bir araştırmaya göre 2015 yılında gençlerin %73'ü cep telefonu sahibiyken, günümüzde % 95 seviyelerine çıkmıştır. Gençlerin %43'ü neredeyse her an çevrimiçi, %44'ü de günde en az birkaç kez bağlanmakta olduğunu beyan etmiştir (Sarıoğlu, 2019: 149-150). Bu doğrultuda gençleri siber tehlikelerden, terör sempatisinden, teknoloji bağımlılığından, mahremiyet yoksunluğundan vs. yaşanabilecek tehditlerden korumanın tek yolu ebeveyn olarak teknoloji ile barışıp hatta teknolojiyi öğrenip bebeklikten itibaren çocuklara internet dünyası hakkında sorumluluk bilinci ve siber tehditlere açık olduğu algısını vermekten geçmektedir.

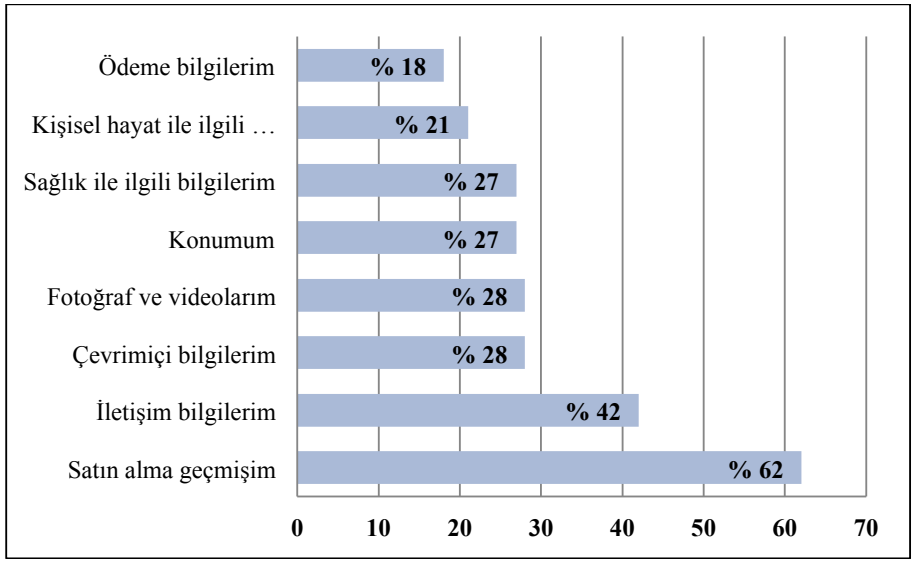
Z kuşağı dediğimiz bizim çocuklarımız torunlarımızdır nihayetinde. Onlar kendi kendilerine bilinçli davranmaya çalışırken anne ve babaların da kendilerine çeki düzen verip çocukları itmemeleri gerekmektedir. Yetimhanelerde çocuklar anne ve baba sevgisi tatmadıkları için onlara iyi davranan kim olursa onun peşinden giderler. Bu kişiler kötülük yapmak ya da yaptırmak amacıyla bile o çocuğa iyi davransa çocuk yine onu takip eder. Buna *yetim çocuk psikolojisi* denir. Ancak günümüzde anne ve babalar kendileri çocuklarıyla ilgilenmeyip aynı koltukta oturup ama ellerinde telefonla vakit geçirirse, çocukla ilgilenmezse o çocuk da başka yerde ilgi arar. Buna da *analı babalı yetim çocuk psikolojisi* denir. Bu çocuklar da sanal alemde ilgi, alaka aramakta, yalnızlıktan dolayı sanal alemde sanal dostluklara inanıp iletişim kurmaya çalışmaktadır (Yakaryılmaz, 2018: 124). Çocuklarımızı kendi ellerimizle itmeyelim, kendimizi de teknolojinin esiri olmaktan kurtarıp örnek ebeveyn olalım. Yoksa çocuklarımızı geri kazanmak için zamanımız olmayabilir.

Ancak daha kontrolsüz olması beklenen Z kuşağı, güvenlik ve tehdit algısı yönünden ihtiyatlı tavırlar sergilemektedir. Bu da umut vericidir. IBM şirketi ve Amerikan Ulusal Perakende Federasyonu'nun ortak yaptığı bir araştırmaya göre kişisel bilgilerin paylaşımı ve kişisel bilgilerin korunması konularında aşağıdaki tablolara bakarak bilinçli oldukları yorumunu yapabiliriz (Sarıoğlu,

2019: 152). Yapılan araştırmada sorulan iki sorunun karşılığında alınan cevapların yüzdeleri aşağıdaki grafiklerde verilmektedir.

Grafik: 2: Z Kuşağının Dijital Ortamda Kişisel Bilginin Paylaşımına Yaklaşımı

Araştırma sorusu: *Hangi bilgiyi en beğendiğiniz marka ile paylaşma konusunda istekli ve rahat olursunuz?*

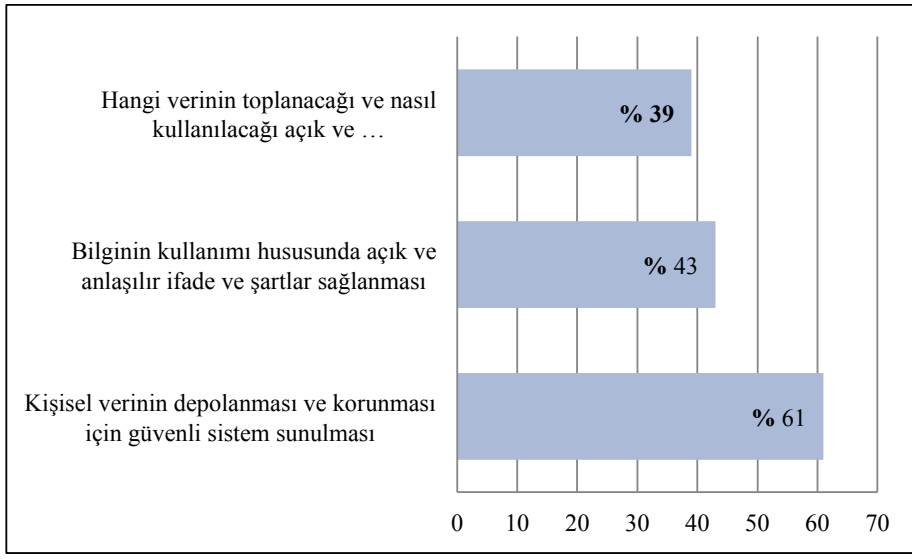


Kaynak: Sarıoğlu, 2019: 152

Yukarıdaki grafiğe göre Z kuşağının yalnızca %18'i ödeme bilgilerini ve yalnızca % 21'i kişisel hayat bilgilerini paylaşabileceklerini açıklamış geri kalanları bunları açıklamayı reddetmiştir. Bu da teknolojinin içine doğan bu kuşağın siber güvenlikten yana bilinç düzeyinin yüksek olduğunu göstermektedir.

Grafik: 3 Z Kuşağının Dijital Ortamda Kişisel Bilginin Korunması Hususunda Öncelikleri

Araştırma Sorusu: *Aşağıdakilerden hangisi kişisel bilgilerinizi markalar ile paylaşım konusunda daha iyi hissetmenizi sağlayacaktır?*



Kaynak: Sarıoğlu, 2019: 152

Yukarıdaki grafiğe baktığımızda Z kuşağının kişisel verilerini paylaşmak için önce güvenmesi gerektiğini anlıyoruz. Güven kriteri de ispatlanabilir, kişisel verilerin korunması ve depolanması için güvenli sistemler kullanılıp kullanılmaması gibi somut güvenlik önlemlerini içermektedir.

4. SİBER MÜCADELENİN İŞ HAYATINDAKİ PROFESYONEL YANSIMALARI

Uluslararası ekonomiye baktığımızda da İnternetin kontrolünü elinde bulunduran Amerika'nın ekonomi trafiğini de kontrol altında tuttuğunu söylemek yanlış olmaz. İnternet devleri Facebook, Twitter, Google, Amazon, Yahoo ve pek çok elektronik ticaret sitesi Amerika merkezlidir. Günümüzde artık eski bankerler, kayseri kasalarında nakit saklayan işletmeler, kazancını altına çevirip evinin sandığında saklasın diye eşine emanet eden esnaflar kalmadı, kalanların da ekonomiyi etkileme gücü kalmadı. Yerine dijital geldi. Yani para artık banka hesaplarındaki rakamlardan, altın borsa değerinden, nakit de banka kartlarından ibaret oldu. İnternet ve internete uyumlu uygulamalar sayesinde ödemeler artık banka hesapları arasında transferler şekilde yapılmaktadır. Son kullanıcının yaptığı ödemeler de havale, eft, kredi kartı, diye sayacağımız seçenekler yine ABD merkezli Visa, Mastercard, Paypal gibi şirketlerin sağladığı

hizmetlerdir. Yani ödeme trafiğinin ağırlığı yine ABD'den geçmekte ve onun kontrolünde yapılmaktadır (Aust ve Amman, 2018: 36).

Ayrıca şirketlerin verilerini saklamak için "Bulut Bilişim" (Cloud Computing) adındaki ucuz bir servis olan saklama merkezi de yine Amerika'dadır (Aust ve Amman, 2018:36). Buraya şirketler, kurumlar, üniversiteler, şahıslar ve her kim isterse veri yüklemektedir. Dolayısıyla kullanımda kolaylık sağlayan fakat çok daha büyük tehditler içeren hizmetlerin merkezinde hep Amerika yer almaktadır. Avrupa, Rusya, Çin ve diğer Uzakdoğu ülkelerinden zaman zaman bunlara ikame yeni sistemler üretilmekte fakat dünya genelinde hâkimiyeti sağlayamamaktadırlar.

Şirketlerin tehdit altında olduğu bir konu da bir devletin kontrolünde olmanın dışında zararlı yazılımlar ve casusluk faaliyetleridir. Örneğin 2000 yılında Yahoo ve eBay gibi dev sitelerin yayınları DDoS saldırısıyla kesintiye uğratılmıştır. 2001 yılında register.com sitesinin DNS sunucularına saldırılmıştır. 2007 yılında Wolfenstation, Counter Strike gibi on binden fazla oyun sunucusu BOTNET ağıyla saldırıya maruz kaldı. 2009 yılında ThePirate Bay P2P sitesinin yayını kesildi. Bunlar uluslararası ticareti ve kullanıcıları etkileyen büyük saldırılardır (Kurgan, 2017: 126-127). Benzerleri ve çok daha yaygın şekli şirketlerin büyüklüğüne bakmadan sürekli gerçekleşmekte ve güvenlik çalışmalarına çok büyük bütçeler ayrılmaktadır.

Güvenlik amaçlı verilerin korunmasına yönelik resmi, ticari ve bireysel olarak toplam bütçelere bakarsak; 2018 verilerine göre küresel olarak bilgi güvenliği harcamalarının toplam bütçesinin 114 milyar dolara çıktığını ve bu rakamın 2022 yılına kadar 1 trilyon doları geçeceği yeni bir piyasanın oluşmuş olduğunu rahatlıkla söyleyebiliriz (Siber Bülten, 2019: 9). Yine de teknoloji uzmanlarının artık genel kabul görmüş düşüncesine göre ne yaparsak yapalım yüzde yüz güvende olduğumuz söylenemez. Bu durumda başka gizlenme yolları üretilmektedir. Önemli bir bilginiz, ihale rakamınız, vergi borcunuz, çalışanınızla olan bir davada kaybedilen tazminat vs. her türlü aleyhinize kullanılabilecek olan bilgiyi saklamanın bir yolu da bilgiyi bilinçli olarak değiştirmektir. Şirket yöneticisi olarak, sakladığınız bilgisayardaki bilgiyi kendiniz bileceğiniz şekilde başka bir ortamda ilişkilendirmeden muhafaza edip, ilişkili evraklarda ya da dosyalarda işiniz bitene kadar farklı rakam, isim, tarih vs. gibi yanlış bilgi yazarak güvende olmaya devam edebilirsiniz (Ahearn ve Horan, 2012: 73-76). Tabi bu da kısıtlı ve hedefe yönelik dosya ya da bilgiler için geçici bir çözümdür. Ancak yakın gelecekteki ihaleyi elinizden kaçırmayı engelleyebilir.

5. SİBER MÜCADELENİN DEVLETLER VE ULUSLARARASI MECRA BOYUTU

Artık cephe savaşları, orduların karşı karşıya göz göze gelerek yaptıkları savaşlar, topu tüfeği askeri çok olanın, üzerine bir savaş stratejisi katarak kazandığı mücadeleler geride kaldı. Soğuk savaş dönemi bile ateş açılmayan bir ateş hattı gibiydi ve siviller dahi bunun bitmesini teyakkuzda beklemişlerdi. Ancak şimdilerde akıl savaşları yapılıyor fakat bunun yansımaları çok sonra oluyor, siviller ve hatta işin içine doğrudan dâhil olmamış olan yan odada çalışan memur ve ordu mensupları dahi bunu hissetmiyor.

Siber saldırılar son yıllarda onlarca kez yapılmıştır. Amerika, İran ve Kuzey Kore silah programlarına; Kuzey Kore Amerikan bankalarına, ünlü bir Hollywood yapım şirketine ve Britanya sağlık sistemine; Rusya, Ukrayna'nın, Avrupa'nın ve Amerika'nın siyasal sistemlerine siber müdahalelerde bulunmak suretiyle siber savaşı tırmandırmışlardır. Ancak neyse ki doğrudan insan hayatına mal olmamış girişimler olarak kalmışlardır (Sanger, 2019: 9). Fakat yeni siber saldırıların, neyle karşılık göreceği devlet yöneticilerinin sağduyusuna bağlıdır.

Terör kelimesinin kökeni Latince *terrere* kelimesidir. Korkutma, yıldırma, tehdit gibi anlamlar içerir. Terörizm ise bunlara süreklilik ve siyasal içerik katmaktır. Siber terörizm ise terör eylemlerinin bilgisayar ve bilgisayar sistemleri kullanılarak yapılmasıdır diyebiliriz. Elektronik ağları ve bilgisayar ve internet teknolojileri silah olarak kullanmaktadırlar. Gelişen teknolojiye bağlı olarak terör de kabuk değiştirmiş ve siber terör doğmuştur. Terör örgütleri ayrıca kendilerine yandaş toplama amacıyla da sosyal medyayı kullanmaktadır. IŞİD terör örgütü pek çok üyesini sosyal medya ağları üzerinden toplamıştır. Ya da virüsler yoluyla yapılan 2010'daki İran Nükleer Santraline yönelik siber saldırı da bir başka teknolojiyi kullanma yollarıdır. Bu siber saldırıyı kimse üstlenmedi. Stuxnet USB ile bulaşan bir virüstür. 30 binden fazla bilgisayarı etkileyerek en sonunda nükleer çalışmalar yapan bilgisayarların çökmesine sebep olmuştur. BBC bu saldırıdan dolayı İran'ın, İsrail ve ABD'yi sorumlu tuttuğunu açıklamıştır (Dağıtmaç ve Ekmen, 2019: 55-58) .

Geleneksel terör ve yeni nesil terör arasında bazı derin farklar vardır. Yeni nesil terörün algılanması, belirlenmesi, önceden önlem alınarak eylemlerin durdurulması, ya da yer konum bilgisi tespiti yapılıp baskın verilmesi gibi önleyici faaliyetler artık çok zor ya da imkânsızdır, hatta çok karmaşık süreçler gerektirebilir yahut da en sonunda çok masum bir kişiyi terör zanlısı ilan edebilirsiniz. Daha da ilerisi, kendiniz bile hem terör kurbanı hem de zanlısı olabilirsiniz. Çok uzak bir yerden terör faaliyeti internet üzerinden yapılıp çok

masum bir kişinin konum ve bilgisayar kimliği açık edilerek başkasına suç bırakılabilir. Bu şekilde görünmez bir tehlike varken kimse tam olarak güvende sayılmaz (Dağıtmaç ve Ekmen, 2019: 58).

Eskiden muhtemel hasımlar belli idi: bunlar devletler ve ordular düzeyindeydi. Şimdilerde ise hasım konsepti de değişmiştir. Siber altyapılar savaş eşiğini düşürerek savaş ve barış arasındaki farkı yok etmiştir. Siz hiç silah sesi duymadan, günlük hayatta gayet mutlu yaşarken birileri sizin enerji kaynaklarınızı, elektrik ve su şebekelerinizi, sağlık ya da trafik kontrol sistemlerinizi ya da herhangi bir ağınızı hack'lemiş olabilir. Bu dönüşüm savaş terimini de dönüştürmüş ve hasım profilini de değiştirmiştir. Artık zarar veren her siber saldırı bir savaş gibi algılanabilir. Ayrıca tüm hackerlar da muhtemel düşman olabilir. Fakat bu genelleme sonsuz ve tespit edilmesi mümkün olmayan bir evreni işaret etmektedir (Schwab, 2018: 95).

Bilgisayar sistemlerimize giren casuslar ve teröristler pek çok kötülük yapabilirler. Uçakların havalanmasını engelleyebilir, silahların ateşlemesini durdurabilir, bir füzeyi hiç istenmeyen bir zamanda ve istenmeyen bir yere gönderebilir, sır sayılacak bilgileri başka istihbarat servislerine gönderebilir, askeri, siyasi planlarımızı öğrenebilir, daha da vahimi planlı ve organize şekilde devletin her kademesine sızarak milletin geleceğini tümden yok etme amacına hizmet edebilirler (Dağıtmaç ve Ekmen, 2019: 60-61). Dolayısıyla savaş ve düşman artık görünmez bir hale büründüğünden tek yapılabilecek olan oyunu kuralına göre oynayarak oyuna dâhil olan değil oyunu kuran olabilmektir. Türkiye'nin de içinde bulunduğu 42 ülkenin imzaladığı silah ihracatını kontrol altına almayı amaçlayan Wassenaar Sözleşmesi; kontrol edilmesi gereken silahlar listesine "internet gözetleme ve sızma yazılımlarını" da eklemiştir (Siber Bülten, 2019; 9). Bu durum bize siber güvenliğin ne derece önemli, devletlerin bu konuya ne derece hassas ve hayatımızı ne derece tehdit ettiği hakkında önemli bir dayanak olmaktadır.

Zararlı yazılımlar ülkelerin kullandıkları en iyi silahlardır. Bunu bazen devlet kontrollü olarak bazen de suç örgütleri kendi menfaatleri için kullanırlar. Türkiye'deki cihazlar donanım olarak yeterince güvenlikli olmadığından ve yasalar ve yaptırımlar da bu güvenlik tedbirlerini almak için yeterli olmadığından internet erişimi olan cihazların yarıya yakını tehdit altındadır. Aşağıdaki tabloda görüleceği gibi; 2018 verilerine göre Türkiye zararlı yazılım barındırma açısından dünyadaki üçüncü güvensiz ülkedir. Cihazlarımızın yüzde kırktan fazlasında zararlı yazılım bulundurmaktadır. Bu da zararlı yazılımı bilgisayarımıza yükleyenlerin kullanımına açık hale gelmesi demektir. Bunda hedef doğrudan kendimiz ve ülkemiz olabileceği gibi, bir ülkeden bir üçüncü ülkeye yapılacak işlemin bizim ülkemizdeki bir bilgisayar üzerinden yapılması

da olabilir. Gerçekte yapanların tespit edilememesi ve araştırıldığında bizim ülkemizden yapılmış olduğunun sanılması yani suçun üzerimize kalması doğacak en vahim sonuçlardan biridir. Bunda hem şahsımız, hem de ülkemiz geri dönülmez sonuçlar ve yaptırımlarla karşı karşıya gelebilir.

Tablo: 2 En Çok Zararlı Yazılım Bulunduran Ülkeler

Sıralama	Ülke	Yüzde
1.	Çin	%49
2.	Tayvan	%47,34
3.	Türkiye	%40,99
4.	Rusya	%38,95
5.	Guatemala	%37,56
6.	Meksika	%36,89
7.	Peru	%36,23
8.	Ekvador	%36,22
9.	Brezilya	%34,68
10.	Polonya	%33,01

Kaynak: Yakaryılmaz, 2018: 47

Zararlı yazılımların neden olduğu birkaç örnek olay vermekte yarar vardır. 2001 yılında İrlanda Ekonomi Bakanlığı sunucuları İrlanda Maynooth üniversite öğrencileri tarafından saldırıya uğramıştır. 2008 yılında Rusya-Gürcistan savaşında, Gürcistan Cumhurbaşkanlığı Sitesi pek çok ulusal devlet sitesi ve Ulusal Bankası Rus korsanlar tarafından saldırıya uğramıştır. 2009 yılında ABD Beyaz Saray resmi sitesi DDoS saldırısı sonucu 3 gün kapalı kalmıştır(Kurgan, 2017:126-127). Bunlara benzer pek çok örnek vermek mümkündür. Amerika'dan yönetilen bir sistemde bile, Beyaz Saray'ın resmi web sitesi zarar görebiliyorsa tüm devletler için tehdit çok büyük boyutlardadır demek yanlış olmasa gerek.

15 Ağustos 2012 Çarşamba günü, İran'a yakın bir grup, piyasa değeri 2 trilyon dolar civarı olan Suudi Arabistan'ın önemli petrol şirketi Saudi Aramco'ya saldırdı. Saldırı bir çalışanın bilgisayara taktığı USB ile bulaşan bir virüs ile yapıldı. Shamoon ve Disttract adı verilen virüs ile verileri silmek amaçlandı. Hatta veriler geri getirilemesin diye dosyalara farklı bilgiler kaydedilerek orijinal dosyada yok edildi. Ardından hackerlar saldırının başarısını açıklamak için, virüs bulaşan bilgisayarların IP adreslerini internette yayınladır. Bir günlük hasar ABD, İsrail ve Rusya ortak çalışması ile 2 haftada kont-

rol altına alınabildi. Yaklaşık 30 bin bilgisayar yani şirketin bilgisayarlarının dörtte üçü çöp olmuştu. Amaç şirketten ziyade ülkeye yönelikti. Eğer petrol arzı dursaydı Suudi ekonomisi büyük zarar görecek, petrol fiyatları yükselecek, ABD'de de petrol fiyatları yükselecek ve dünya İran petrolüne başvurmak isteyecekti. Böylece İran ambargosu kaldırılmak ve İran petrolü kullanıma sunulmak zorunda kalınacaktı (Ross, 2017: 125-127). Sadece bir çalışanın kontrolsüz (ya da bilinçli) bir şekilde bilgisayara taktığı bir USB bir ülkenin geleceğini ve dünyadaki dengeleri değiştirebilirdi. Siber dünya bu denli tehlikeli fakat bu denli de kontrolü güç ve tedbir alması zor bir dünyadır. Sorumluluk bilinci her şeyin önüne geçebilecek tek güçtür.

Türkiye'de ise 2008 yılında Erzincan'ın Refahiye İlçesi Yurtbaşı Köyü mevkiinden geçen Bakü-Tiflis-Ceyhan petrol boru hattı patladı. Sebebi bir siber saldırıydı. Operasyon merkezinin bilgisayarlarına sızılarak uyarı sensörleri devre dışı bırakılmıştı. Borulara gelen fazla petrolü sensörler algılayamadığı için patlama kaçınılmaz olmuştur. Hattın tekrar devreye alınması 3 hafta sürdü. Günlük 1 milyon varil petrolün Hazar Denizi'nden Akdeniz'e ulaştırıldığı bu hattaki olay sonucu Türkiye günde 500 bin dolar, BP ve ortakları günde 5 milyon dolar, Azerbaycan ihracatı da 1 milyar dolardan fazla para kaybetmiştir. Ayrıca olay sonucu çevreye 30 bin varilden fazla petrol saçılarak doğada da tahribata yol açarak bölgenin ekolojisini de bozmuştur (Kurgan, 2017: 33-34).

SONUÇ YERİNE BİR DEĞERLENDİRME

Buraya kadar anlattığımız, deryanın içinde bir damladır sadece. Bu sebeple tedbirler olay başımıza geldiğinde bertaraf etme üzerine olmamalı, olay başımıza gelmeden önleyici olmalıdır. Çünkü siber suçlara maruz kaldığımızda müdahale etmek yani reaktif çözüm bulmak çok zordur. Onun yerine proaktif bir yaklaşımla plan yapmak ve öngörülerde bulunarak önleyici tedbirler almak gerekmektedir (Pazoğlu ve Yücesoy, 2019: 1).

Günümüzde verilerimizi korumak için bazı tedbirler yaygınlaşmıştır. Bunların içinde güçlü ve güvenli şifreler kullanma sürekli yenileme, güncellemeler, yamalama, sıkılaştırma, güvenlik duvarları ve saldırı önleme sistemleri vb. tedbirler yer almaktadır. Bunların bilinip kullanımının yaygınlaşması önem arz etmekle beraber yeni saldırı modelleri o kadar hızlı üretilmektedir ki bunlar da ciddi korunması gereken durumlarda yeterli olmayacaktır. Burada detayına girilmeyecek olan hedefli saldırılar (APT) ya da 0. Gün (zeroday) gibi saldırılar yine teknik detayı başka bir çalışmanın konusu olan aktif savunma kavramının gerekliliğini ve önemini ortaya çıkarmaktadır (Pazoğlu ve Yücesoy, 2019:19). İleri boyutta siber güvenlik çalışmalarında aktif savunma yöntemleri incelenebilir.

Kişiliğimizi korumanın ötesinde içinde bulunduğumuz toplumu da korumak bilinçli vatandaşın görevidir. Bireyler, tek tek, ya da grup halinde, sivil toplum örgütleri ya da sivil platformlar şeklinde dördüncü sanayi devriminin getirdikleri ve götürebilecekleri üzerine toplumu uyarıcı, eğitici, bilinçlendirici çalışmalar ve etkinlikler yapabilir. Böylece teknik adamlar da ürettikleri teknolojinin insanlığı nereye götürdüğünü belki daha iyi anlayarak ve anlatarak yeni üretecekleri teknolojiler hakkında daha kapsamlı düşünerek hareket edebilirler (Schwab, 2019: 315).

Devlet olarak kendi teknolojimizi üretme konusu iktisadi olarak da zorunludur. Robotik ve yapay zekâya devlet ve özel sektör birlikte önem vermelidir. Özel sektörce robotlarla ikame edilecek işler için kaynak ayrılması, devletin robotik ile ilgili engelleri ortan kaldırıp yasal düzenlemeleri gözden geçirmesi, sendikaların işçi-robot birlikteliği üzerine projeler üretmeleri ekonomimizi hızla yukarı çekebilir (Akın, 2017: 71). Bu sayede kendi yazılımlarımızı ve kendi siber uzayımızı kurabilir, dolayısıyla ithal mal ve hizmetten kaçınarak güvenliğimizi bir nebze daha koruyabiliriz.

Örneklerde görüldüğü üzere tek bir USB girişi bütün dünyayı etkilerken, sosyal medya bizi ele geçirmişken, evdeki buzdolabı bile casus olmuşken kendimizi ve dünyayı korumak için neler yapılabileceğini ve neleri yapmamak gerektiğini öğrenmeye çalışmak ve bu doğrultuda kafa yormak en büyük vazifemiz haline gelmiştir.

KAYNAKLAR

AHEARN, Frank .M. ve HORAN,Elieen.C. (2012). İz Bırakmadan, (Çeviren: A.Pardo) İstanbul: NTV Yayınları.

AKIN, Ömer. (2017). *Hızla Artan Endüst7riyel robotların Üretim Süreçlerinde Yarattığı Değişimler ve Türkiye İşgücü Piyasasında Yaratacağı Olası Etkilerin Değerlendirilmesi*, İş ve Hayat Dergisi, 6: 71.

AUST, Stefan ve AMMANN Thomas. (2018). ***Dijital Diktatörlük***, (Çeviren: E. Yücel ve H. Yılmaz), İkinci Baskı, Ankara: Hece Yayınları.

BAŞARAN, Alper. (2019). ***Zararlı Yazılımlar***, İstanbul: Arion Yayıncılık.

CANAN, Sinan veACUNGİL, Mustafa. (2019). ***Dijital Gelecekte İnsan Kalmak***, Dördüncü Baskı, İstanbul: Tuti Kitap.

DAĞITMAÇ, Murat ve EKMEN, Şehadet. (2019). ***Dijital Psikolojik Devrim***, İkinci Baskı, İstanbul: Motto Yayınları.

ERDOĞAN, Yavuz. (2012). ***Türk Ceza Kanunu'nda Bilişim Suçları***, İstanbul: Legal Yayıncılık.

ERDOĞAN, Yavuz. (2018). ***Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri***, İstanbul: Legal Yayıncılık.

EREN, Mehmet. (2017). ***Avrupa Birliği'nin Siber Güvenlik Politikası***, İstanbul: Beta Yayıncılık.

FALKNER, Brian. (2012). ***Akıl Hırsızı***, (Çeviren: B. Yılmazcan), Ankara: Akılçelen Kitaplar.

HERZBERG, Caspar. (2017). ***Akıllı Şehirler Dijital Ülkeler***, (Çeviren: N. Özata), Optimist Yayınları.

KURGAN BİLİŞİM GÜVENLİĞİ ARAŞTIRMALARI VE GELİŞTİRME MERKEZİ, (2017). ***Siber Mücadeleye Giriş***, İstanbul: Kutlu Yayınevi.

PAZOĞLU, Evren ve YÜCESOY, M. Nezir. (2019). ***Siber Güvenlik Operasyonları Merkezi*****,** Ankara: Gazi Kitabevi.

ROSS, Alec. (2017). ***Geleceğin Endüstrileri***, (Çeviren: M. Buğan), Ankara: Orion Kitabevi.

SANGER, David.E. (2019). ***Mükemmel Silah Siber Çağda Savaş, Sabotaj ve Korku***, (Çeviren: J. C. Yapıcıoğlu), İstanbul: Profil Kitap.

SARIOĞLU, E.Başak. (2019). *Kuşaklar ve Halkla İlişkilerin Dijital Evrimi*, SARIOĞLU E.B (Editör) ***Dijital Halkla İlişkiler***, Konya: Eğitim Yayınevi, 146-153

SCHWAB, Klaus. (2018). ***Dördüncü Sanayi Devrimi***, (Çeviren: Z. Dicleli), İstanbul: Optimist Yayınları,16,17, 95

SCHWAB, Klaus. (2019). ***Dördüncü Sanayi Devrimini Şekillendirmek***, (Çeviren: N. Özata), İstanbul: Optimist Yayınları, 315

SİBER BÜLTEN. (2019). *Siber Bülten*, **Arka Kapı Dergisi**, 9: 9

ŞEKER, Selim. (2018). ***5G Nesnelerin İnterneti ve Salığımız***, İstanbul: Hayy Kitap, 164

TURHAN, Gökhan ve OKCU, Murat. (2018). ***Siyasette Dijital Yerliler ve Göçmenler***, Ankara: Gece Kitaplığı, 140-150

YAKARYILMAZ, Faruk. (2018). ***Teknoloji Fırsat mı? Tuzak mı? Ailede Güvenli İnternet Kullanımı***, İstanbul: Oku-Yorum Yayınları, 47, 124

YILDIZ, Sevil. (2007). ***Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi***, Ankara: Nobel Yayın Dağıtım, 35