Konu: **Bilim**
Yazı: **61**

Bilgi Çağının Sorunları

Doç. Dr. Haluk Berkmen

1800'lü yıllarda başlayan endüstri çağı son 40 yıldan beri yerini bilgi çağına bırakmıştır. Bu çağı oluşturan devrim bilgisayar teknolojisinin yaygınlaşarak evlere girişidir. Hele internet denen elektronik iletişim ağı kurulduktan sonra bilginin aktarılması ve yaygınlaşması akıl almaz bir hız kazanmıştır. Herkesin kullandığı cep telefonları ve taşınabilir (laptop) bilgisayarlar **mikroçip** sayesinde gerçekleşmiştir. Bir ***entegre*** (birleşik) devre olan mikroçip 1958 yılında elektrik mühendisi **Jack Kilby** (1823 – 2005) tarafından icat edilmiştir. İlk ticari taşınabilir bilgisayarı IBM şirketi **IBM 5100** adıyla 1975 yılında piyasaya sürdü. Bundan sonra yaygınlaşan taşınabilir bilgisayarlar modern bilgi çağının hızla gelişmesini sağladı. Günümüzde cep telefonları ve tablet denen dokunmatik ekranlı bilgisayarlar yaygın şekilde kullanılmaktadırlar.

Bilgi çağının yararları olduğu kadar zararları da vardır. Sadece yararları görüp bilgi çağında ortaya çıkan zararlı etkileri ve sonuçları görmezden gelmemeliyiz. İnternet sayesinde insanlar bir yandan bilgi ve fikir paylaşırken diğer yandan ***dezenformasyon*** denen yanlış ve zararlı olabilecek bilgiye de açık oluyorlar. Dezenformasyon, gerçeği örtmek veya çarpıtmak için ve bir bakıma beyin yıkamak için yayınlanan, duyurulan ve dağıtılan yanlış bilgiye denir. Günümüzde gerek kişilere gerekse toplumlara kasıtlı olarak yanlış bilgi aktarılmakta, istenilen amaca doğru yönlendirilmektedir. Bu tür yanlış bilgi dağıtımına **toplum mühendisliği** de denmektedir.

Elektronik iletişim insanları ve özellikle gençleri yalnızlaştırmış, yüz-yüze fikir alışverişini ve fiziksel teması azaltmıştır. Sosyal medyada binlerce arkadaşı olan fakat hiç biriyle yüzü-yüze karşılaşmamış olan pek çok genç vardır. Günümüzde dünya nüfusunun % 50si şehirlerde yaşamaktadır. Önümüzdeki 30 yıl içinde bu oran % 70lere varacaktır. Ne kadar birbirimize yakın yaşarsak o kadar kendimizi yalıtmak gereğini duyarız. Fiziksel yalnızlaşma sanal bir gerçeklik yaratmakta, sanal insanların sanal dünyası oluşmaktadır. Sonuç olarak sadece kişi kendini gizlemekle kalmamakta, ayrıca kişilik kaybına da uğrayabilmektedir.

Bilgi çağında gittikçe önem kazanan bir diğer oluşum elektronik savaş ve uzaktan kumandalı silahlardır. Elektronik savaş bilgisayarlara bulaşan virüslerle başladı. Bilgisayar virüsü haberimiz olmadan bilgisayarımıza yüklenen bir küçük program veya bir dizi elektronik emirdir. Bu tür virüsler kendilerini kopyalayarak tüm hafızayı doldurabilirler ve bilgisayarın durmasını sağlayabilirler. Daha tehlikeli olanlar bilgisayardaki önemli bazı bilgileri bozabilirler veya silebilirler. Üstelik bilgileri bilgisayarımızdan çalarak diğer bir bilgisayara da aktarabilirler.

Günümüzde ***hacker*** denen bilgisayar hırsızları bilgisayarların güvenlik şifrelerini kırarak gizlice bilgi ediniyorlar, programları durduruyorlar veya tümüyle bozuyorlar. Ayrıca ülkelerarası ***siber savaş*** denen casusluk ve saldırı içeren bir yeni savaş türü geliştiriyorlar.

Siber sözü 1948 yılında Amerikalı matematikçi **Norbert Wiener** (1894 – 1964) tarafından ileri sürülmüş olan **sibernetik** sözünün kısaltılmış halidir. Siber savaşa örnek olarak İran'ın zenginleştirme tesisine İsrail'in 2010 yılında yolladığı STUXNET adlı virüs gösterilebilir. Bu virüs uranyum zenginleştirilmesinde kullanılan birçok santrifüj aletinin durmasını hatta kırılıp çalışamaz duruma gelmesini sağlamıştır. STUXNET herhangi bir ülkeye veya herhangi bir fabrikaya yöneltilebilecek yapıdadır ve tüm iletişim şebekesini durdurabilecek güçtedir. 1 Haziran 2011 tarihli **New York Times** gazetesi bu STUXNET virüsün Amerika ile İsrail'in ortak çalışması sonucunda oluşturulduğunu ve başkan Barack Obama döneminde daha da geliştirildiğini iddia etmiştir. Artık bu tür elektronik virüsleri ***kitle imha silahları*** sınıfından saymak gerekmektedir, zira zararları bir kişiye değil, tüm bir topluma olabilmektedir.

Bilgi çağında ortaya çıkmış olan bir diğer silah da pilotsuz uçan araçlardır (PUA). Bunlara ***drone*** denmekte ve çeşitli boylarda olabilmektedirler. Uzaktan kumanda edilebilen bu araçlar küçük uçaklar veya küçük helikopterler şeklindedirler. Örneğin, Amerika'nın bir laboratuarından yönetilen bir PUA Afganistan'ın istenilen bir noktasını veya bölgesini bombalayabilmektedir. Elektronik oyuna benzeyen bir ekran başında oturan genç, oyun oynar gibi gerçek insanları öldürebilmekte ve saldırdığı bölgeye hiç gitmemiş olduğundan, ne üzüntü ne de vicdan azabı duymaktadır. PUA sayesinde istenilen yerden bilgi toplamak ve hiç asker kaybına uğramadan saldırıda bulunmak mümkün olmaktadır. Saldırıda bulunan ülke için iyi gibi görünse de sonuç itibariyle katı ve vicdansız, acımasız bir nesil ortaya çıkmakta, "**insanlık**" denen değerler yumağı, büyük çapta yozlaşıp anlamını kaybetmektedir.

Bilgi çağının bir diğer elektronik casusluk aracı uzaya atılmış olan uydulardır. Bu uydulara yerleştirilen hassas kameralar sayesinde yeryüzünde istenilen bir noktaya odaklanarak net fotoğraflar çekilebilmektedir. Böylece ülkelerin belli bir alanda –örneğin nükleer silah üretiminde- ne gibi faaliyetlerde bulundukları da izlenebilmektedir. Günümüzde bu fotoğrafları inceleyen ve ülkeler hakkında ayrıntılı raporlar düzenleyen uzman grupları vardır. Bu raporlara dayanarak etkin saldırı planları da yapılabilmekte, siber savaş etkin fiziksel -maddi silahlı- savaşa dönüşebilmektedir.

Elektronik savaşın bir diğer yönü de istenilen kişilerin cep telefonlarının dinlenebilmesi ve tüm e-postalarının kaydedilebilmesidir. İlerde bu bilgiler sayesinde önleyici veya durdurucu tedbirler alınabilir. Bu tür etkin ve önleyici savaş tekniklerine ***proaktif siber savunma*** adı verilmektedir. Prokatif siber savunma oldukça yeni bir terimdir ve 1995 yılında başlatılmış bir programdır. Amacı, terör olayı gerçekleşmeden erkenden fark edip, terörist saldırısını önlemeye dönüktür. Ancak, bu gücü ellerinde bulunduran ülkeler sadece teröristleri değil, ülkenin önemli yöneticilerini veya iş adamlarını da dinlemektedirler. Bu gücün nerelere kadar uzandığını henüz bilmediğimiz gibi, verebileceği zararlardan da habersiziz. Henüz gerçekleşmemiş ve olması mümkün fakat kesin olmayan olaylara önceden tedbir almak ve insanların özel hayatına karışmak ne derece doğrudur? Toplanan bilginin şantaj için veya kötü kişilerin karanlık emelleri için kullanılmayacağını kim garanti edebilir?

Son olarak elektronik kontrol ve etkileme tekniklerinin reklam endüstrisinde kullanıldığını ve beyin yıkayarak insanları daha fazla tüketmeye yönlendirdiğini söylemek isterim.