Bu makale 16 Kasım 2014 tarihinde http://akademikperspektif.com/2014/11/16/siber-suclar-siber-guclere-karsi/ adresinde yayınlanmıştır.

Yrd. Doç. Dr. Serdar YILMAZ
İstanbul Arel Üniversitesi
Uluslararası İlişkiler İngilizce Bölümü

Siber Suçlar Siber Güçlere Karşı

Günümüz insanı teknolojinin baş döndürücü hızıyla birlikte iletişim olanaklarından sonuna kadar istifade edebilmekte ve içinde bulunduğumuz evrenin her bir noktasına evinde kurulu bir bilgisayar ve elindeki cep telefonu aracılığıyla gidebilmekte, dünyanın öbür ucundaki bir olayı canlı canlı izleyebilmektedir. Lakin teknolojik gelişmelerle yaşam koşulları gittikçe iyileşirken diğer taraftan da dengeler değişmeye başlamıştır. Bilişim devriminin pozitif yanlarının tadını çıkaran insanlar, bu devrimin negatif etkilerinden biri olan yeni bir suç türü ile tanışmıştır. Bu suç türü cyber crimes denilen s**iber suçlardır.**

Önceleri küçük topluluklar halinde yaşayan insanlar kullandıkları basit nitelikte aletler ile kayıpların az olduğu küçük çaplı savaşlar yapabiliyorlardı. Teknolojik gelişmeler ile maalesef bu savaşlar bölgesel ve hatta tüm dünyayı etkileyen boyutlara ulaşmıştır. Füzelerin nükleer başlıklarla yüklenmesi, bunlara enerji sağlayan atom santrallerinin kurulması, füzelere yön veren radyo frekanslarının sağlanması ve bilgisayar kontrollü savaş sistemlerinin yaygınlaşması beraberinde milyonlarca insanın ölümüne ve göçüne neden olmuştur. Geçtiğimiz 25 yılda bilişim teknolojisi önceleri ofis süreçlerini kolaylaştırmaya yarayan bir araçken, şimdilerde sanayi, yönetim, ekonomi, ve askeri teknolojinin stratejik bir aracı haline gelmiştir. Herhangi bir suçun elektronik ortamda işlenebilir olması ve bu fiilin hukuka aykırı bir suç olarak tanımlandığı bilgisayar ve ağ sistemleri yoluyla işlenen siber suçlar, 11 Eylül'den önce sadece küçük uzman grupları tarafından tartışılırken, 11 Eylül'den sonra birbirlerine daha da bağımlı hale gelen toplumlar açısından ciddi sorunlar yarattığı anlaşılmıştır.

Önceleri topla tüfekle yapılan savaşlar şimdilerde bilgisayar üzerinden yapılmaya başlanmıştır. Daha çok bilgi sızdırma, çalma ve değiştirme neticesinde ortaya çıkan siber suçlar, tıpkı Wikileaks'te olduğu gibi ülke veya ülkelere yönelik olmak üzere; politik, askeri veya ticari amaçlı olarak kişileri, kurumları ve örgütleri de hedef alabilmektedir. Siber suçların özellikle şahıslara ve kurumlara yönelik olduğunu söylerken insanlığı ne gibi tehlikelerin beklediğinden de bahsetmek zaruridir. NATO'ya göre değişik IP adreslerinden yoğun istek gönderisi sonucunda sunucuların işlem dışı kalması, çok sayıda e-posta

yollayarak sistemi yavaşlatmak ve karşı taraftaki bilgileri çalmak siber suçların bazılarındandır.[1] Dolayısıyla bunların gerçekleşmesi durumunda elektrik kesintileri, uçakların kalkış yapamaması, nükleer santrallerin zarar görmesi ya da askeri birimler arasındaki iletişimin kopması gibi çeşitli sorunlar ortaya çıkarabilir.

İçinde bulunduğumuz 21. Yüzyılda topla, tüfekle ve tankla bir 3. Dünya savaşının olacağı ihtimali çok uzakken siber suçların ve siber saldırıların bu yüzyılın en önemli sorunu olacağı Soğuk Savaş sonrası kendisini belli etmiştir. Özellikle çok gelişmiş ülkelerin ulusal bilgi sistemleri, özel sektör, kamu kurumları, bankalar ve büyük şirketler siber saldırıların hedefi haline gelmişlerdir. Bilgisayar sistemlerinin çökertilmesi, banka hesaplarının boşaltılması, vergilerin silinmesi, sahtecilik, dolandırıcılık ve tehdit gibi yollarla milyarlarca dolar maddi kayba neden olunmuştur. Zaten genel olarak baktığımızda siber suçların belli başlı ortak özellikleri vardır. Bu tür suçların işlenmesinde bilgisayar sistemleri ve teknolojilerinin kullanılması, gerekli kanun ve düzenlemelerin eksik ve yetersiz olmasından ve bu fiilleri karşılayacak ceza normunun bulunmamasından dolayı yakalanma riskinin çok az olması, bu suçun sonucunda büyük paraların kolay ve risksiz olarak temin edilmesi ve zarara uğrayanların (büyük şirketler ve işletmeler) itibar ve prestij kaybetme korkusu nedeniyle seslerini çıkarmamalarıdır.[2]

Durumun en ilginç yanı özellikle kamu kurumlarının ve özel şirketlerin bu saldırılara karşı koyacak %100 güvenli bir önlem alamamış olmalarıdır. Zira İngiltere'de 2001 yılında 172 büyük kurum ile yapılan bir araştırmada, bu şirketlerin hepsinin bir siber saldırıya maruz kaldıkları ve maalesef bu kurumlara karşı kurumlarını koruyamadıkları ortaya çıkarılmıştır. Başka bir örnek vermek gerekirse: 2000 yılında Filipinli bir bilgisayar öğrenci tarafından yaratılan Love (aşk) isimli bilgisayar virüsü Microsoft firmasının Outlook yazılımındaki açığı kullanarak tüm dünyaya yayıldığı için hem pek çok kullanıcıya zarar vermiş, hem de firmanın itibarını zedelemiştir. Aradan geçen kısa zaman sonrasında hackerlerin Microsoft firmasının bilgisayarlarına girmeyi başardıkları ve gizli bilgiler ile ürünlerine ait taslakların çalınmış olabilecekleri tüm dünyaya yayılmıştır. Yapılan bu saldırı bilgisayarların ve kullanıcıların ne kadar büyük tehlike altında olduklarını göstermiştir. Zira bu virüs hızla yayılarak tahminlere göre 18 saat içinde tüm dünyada 100 milyon bilgisayarı etkilemiştir. Etkilenenler arasında dünyanın çok önemli kuruluşları hatta Pentagon, Beyaz Saray ve BP gibi isimler de vardır.

---

[1] NATO, Cyber Defence, http://www.nato.int/cps/en/natohq/topics_78170.htm? Erişim Tarihi, 30.07.2015.
[2] Mehmet Özcan, "Siber Terörizm ve Ulusal Güvenlik: İnternet ve Hukuk", İstanbul: Bilgi Üniversitesi Yayınları, 2002.

Yada örneğin 11 Eylül terör saldırılarını bir siber saldırı olarak niteleyenlerin olduğu gibi böyle görmeyenlerde vardır. Bende 11 Eylül'ün bir siber saldırı olduğunu düşünüyorum, çünkü özellikle Pentagon'un kesinlikle kırılmaz denilen güvenlik şifrelerinin kırılması, hava radar sistemlerinin devre dışı kalması sayesinde iki uçağın gökyüzünde süzülmesi, kaçırılan uçaklardan kaçırılma sinyalleri alınamaması gibi unsurların toplamı bunun en azından teknolojinin bir nebzede olsun kullanıldığı bir siber eylem olduğunu göstermektedir.

Ancak şunu da unutmamak gerekir ki bilgisayar, internet ve iletişim teknolojilerinden faydalanılarak işlenen bilişim suçları ile mücadele etmek oldukça zor ve pahalı bir iştir. Yeterli teknik bilgiye sahip personel ve bu personelin ihtiyacı olan teknik alt yapıya sahip olmak bu suçlarla mücadele edebilmenin olmazsa olmaz koşuludur. Bilişim suçlarıyla mücadelede karşılaşılan temel sorunlar; suçu işleyen kişinin, suçun işlendiği yerin, suç işlenen cihaz ya da sistemin ve suçun ne zaman ve nasıl işlendiğinin tespitinin zor olduğu şeklinde sıralanabilir. Ayrıca bilişim suçlarıyla mücadelenin temel dayanağı ve olmazsa olmazı olan yeterli mevzuat da (kanun, tüzük, ve yönetmelik gibi) göz ardı edilmemelidir. İnternetin olduğu her yerde muhakkak hukuk kuralları etkin şekilde işle(til)meli ve siber suçlar cezalandırılmalıdır. Örneğin yukarıda bahsettiğim Aşk isimli bilgisayarlara ve sistemlere büyük zararlar veren virüsün yazarı, Filipinler'de o dönemde böyle bir suçu tanımlayan ve cezalandıran yasanın bulunmaması nedeniyle serbest kalmıştır. Bu olaydan sonra Filipin Hükümeti dünyanın en kapsamlı bilişim yasalarını hazırlamıştır. Ülkeler arasında işbirliği yapılmalı ve siber suçlara karşı iletişim içinde olunmalıdır. Her ülkede siber suçların cezası çok ağır olmalı ve eğer yoksa ülkeler arasında siber suçlar ile ilgili hukuki bağlar ivedilikle kurulmalıdır. Yani internet nasıl ki uluslararası bir niteliğe sahipse bu suçlar ile mücadelede uygulanacak hukuk kuralları da evrensel olmalı ve herkesin üzerinde mutabık olduğu küresel yasal bir sistem olmalıdır. Eğer bilişim devriminin de bir sınırı olması gerekiyorsa bu sınır her ülkede uygulanacak olan evrensel normlar olmalıdır. Her ülke kişisel verilerin korunmasına dair düzenlemeler yapmalı ve iç hukuklarını da buna göre ayarlamalıdırlar.

Kaynakça

Philip P. Hallom, "Preventions Strategies For The Next Wave Of Cyber Crime", Network Security, October 2005.

Timur Demirbaş, Kriminoloji, Seçkin Yayınları, Ankara, 2005.

Bu makale 16 Kasım 2014 tarihinde http://akademikperspektif.com/2014/11/16/siber-suclar-siber-guclere-karsi/ adresinde yayınlanmıştır.

Faruk Örgün, Küresel Terör, Okumuş Adam Yayıncılık, İstanbul, 2001.