Siber Dünya

"Gerçeklik" ve Reel Tehditler

Bilişim teknolojilerine olan bağımlılık her alanda giderek artıyor. Bu durum ise siber uzayın düzenlenmesini, denetlenmesini, güvenliğinin sağlanmasını ve bu alanda ortaya çıkan yeni aktörler arasında güç dengesinin tesisini zorunlu kılıyor.

Oğuz Kaan PEHLİVAN

Hayatın her alanına gün geçtikçe daha çok nüfuz eden bilişim teknolojileri birtakım yenilikler ve değişimler getirmenin yanı sıra, tehdit ve güvenlik algılarını da değiştiriyor. Mekanik teknolojiden dijital teknolojiye geçiş ve gerçeklik-soyutluk dikotomisiyle özdeşleştirildiğinde modernizmin gerçekliği üzerine bir soyutluk ve belirsizlik inşa eden post-modernizm, bilişim teknolojilerinde tam anlamıyla bir "gerçeklik" buluyor. Sahip olduğumuz bilgisayar teknolojisi kablolar, çipler ve mikro çipler, pikseller ve donanım malzemelerinin ötesinde bizlere farklı bir dünya sunuyor. Bu dünyanın gerçek olana paralel, ancak *sui generis* (kendine özgü) bir yapıda ve çok farklı kuralları mevcut. Siber uzay tabir edilen bu alan, günlük yaşamın vazgeçilmez bir parçası hâline gelen akıllı telefon, tablet ve masaüstü bilgisayarlarla bağlandığımız internet ağı üzerinde gerçeklik imkânı buluyor. Bankacılık işlemleri, finansal hareketler, bilgi paylaşımı, resmî işlemler gibi pek çok iletişimsel faaliyet ve hizmet siber uzayın konusu hâline gelmiş durumda. Kısacası bilişim teknolojilerine bağımlılığımız her alanda giderek artıyor. Bu durum ise siber uzayın düzenlenmesini, denetlenmesini, güvenliğinin sağlanmasını ve bu alanda ortaya çıkan yeni aktörler arasında bir güç dengesi tesisini zorunlu kılıyor. Bu açıdan konunun güvenlik boyutuyla ele alınması oldukça önemli.

Bilgi güvenliği, kısaca, bilginin "gizlilik", "bütünlük" ve "erişilebilirlik" unsurlarının korunması olarak tanımlanır. Örneğin; bir saldırgan internet bankacılığı hesabınızı ele geçirdiğinde "gizlilik", verileri değiştirdiğinde "bütünlük", sisteme erişimi engellediğinde ise "erişilebilirlik" zarar görmüş olur. Temel hedefi bu üç unsuru korumak olan siber güvenlik, siber ortamdan gelebilecek tehdit ve saldırılara karşı geliştirilen politikalar, stratejiler, risk yönetimleri vb. yaklaşımları içermekte. Bu bağlamda siber güvenlik başlığı altında dört alt kavram da mercek altına alınmış durumda: *siber suçlar, siber saldırılar/savaş, kritik altyapı güvenliği ve siber istihbarat*. Günümüzde devletler için yeni bir mücadele ve üstünlük sağlama alanı olan siber uzayda kişilerin (yani sanal ortamda depolanan kişisel verilerin), kurumların (kurumsal bilgi güvenliği, veri tabanı güvenliği) ve sistemlerin (özel veya kamu girişimi olan kritik altyapıların-enerji, su, iletişim, ulaştırma, finans vb. sistemlerinin) korunması adeta bir zorunluluk.

Sanal dünyada gerçek tehditler

Siber suçlar bilişim suçları, banka ve kredi kartı dolandırıcılığı ve nitelikli internet dolandırıcılığının yanı sıra bilişim sistemleri aracılığıyla işlenen özel hayatın gizliliği, hakaret, tehdit, şantaj, narkotik ve terör suçları ile çocuklara yönelik suçları kapsıyor. Bu suçlar klasik suçların kat be kat ötesinde etkilere sahip ve kolaylıkla sınır aşan bir niteliğe bürünebilir hâlde.

Öte yandan konvansiyonel silahların ve savaşların yerini -şimdilik tamamlayıcı nitelikteki- siber silahlar, saldırılar ve savaşlar almaya başladı. Nitekim Estonya, *siber saldırı* konusunda akla gelen ilk çarpıcı örneklerden. Estonya'nın Nazi işgali karşısında Sovyet askerlerinin verdiği mücadeleyi sembolize eden Bronz Asker Heykeli, 2007 yılında bulunduğu yerden kaldırılmıştı. Heykelin kaldırılması, Rusya tarafından kınandı, ülkede çeşitli gösteriler düzenlendi. İlk olarak bazı devlet siteleri ele geçirilerek başlangıç seviyelerde *yığın e-posta (spam)* ve *DDoS* (bilgisayar sunucusunu aşırı yüklenme sonucu devre dışı bırakma) saldırıları düzenlendi. Sonraki günlerde ise ulusal bilgi sistemlerini, internet hizmet sağlayıcıları, banka ve finansal kurumları, *kritik altyapıları* hedef alan daha kapsamlı ve organize *DDoS* saldırıları gerçekleştirildi. Öyle ki ülkede internet altyapısı çökme noktasına geldi.



Aslında yapılan saldırılar, internet altyapısı ve web sitelerini hedef almanın ötesinde bir anlama sahip. Çünkü Estonya internet ve bilişim sistemlerine yüksek oranda bağımlı bir ülke. Vergi işlemlerinin yüzde 80'i, bankacılık işlemlerinin ise yüzde 97'si internet üzerinden yapılıyor. Sağlık verilerinin tamamı dijital ortamda tutulurken her dört şirketten biri internet üzerinden kuruluyor. 1,3 milyon nüfusa sahip Estonya'da dijital kimlik kartı kullanıcılarının sayısı ise 1 milyondan fazla. Dolayısıyla, ülkede hayatı durma noktasına getiren 2007 tarihli *siber saldırılar* ciddi ekonomik ve sosyal sonuçlar doğurmuş durumda.

İran'ın *kritik altyapısı* olan nükleer sistemlerine saldırı amaçlı özel olarak tasarlanan STUXNET virüsü ise siber silah konusunda ilk akla gelen örnek. Hatırlanacağı üzere STUXNET virüsü, İran'ın uranyum zenginleştirme faaliyeti yürüttüğü nükleer santrali hedef almış ve bilgisayar sistemine sızarak SCADA olarak adlandırılan uzaktan kontrol sistemlerine fiziksel zararlar vermişti. Böylelikle İran'ın nükleer çalışmaları en az 1,5-2 yıl gibi bir süre geriye gitmiş oldu.

Bir başka dikkat çeken konu ise *siber casusluk/istihbarat* faaliyetleri. APT (Gelişmiş Kalıcı Tehdit) olarak adlandırılan *siber casusluk* faaliyetleri aracılığıyla özel hedefler için tasarlanan araçlar yardımıyla hedef sisteme girmek, uzun yıllar boyunca sistemden kendisini gizleyerek bilgi sızdırmak mümkün. *Mandiant Intelligent Center* raporuna göre Çin, 2003 yılında başlayan ve "Titan Yağmuru" olarak adlandırılan *siber casusluk* faaliyeti sonucunda Amerika'nın kritik finansal, ekonomik ve askerî tesislerinden terabaytlarca kritik bilgiyi ele geçirdi. Hatta *Time* dergisinin Amerika baskısında yer alan 2005 tarihli bir analiz, Çin'in 2004 yılında gayrisafi yurt içi hâsılasında yakaladığı 9,1 oranındaki reel büyümenin bu faaliyetler sonucu elde edilen bilgilerin işletilmesiyle gerçekleştiği yönünde iddialara sahip.

Türkiye'nin ihtiyaç duyduğu strateji

Fiziksel sınırların yok olduğu, düşük maliyetli araçlarla büyük zararlar verilebilen ve saldırganın kimliğini gizlenmesini mümkün kılan böylesi bir ortamda, ulusal siber güvenlik stratejileri belirlenmesi ve uygun/etkili mücadele araçlarının hayata geçirilmesi elzem. Türkiye bu alanda etkili olabilmek adına birtakım adımlar attı; ancak bunlar henüz yeterli seviyede olmadığı gibi kat edilmesi gereken daha çok mesafe bulunuyor. Yine de *Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin 2012 tarihli Karar*, Siber Güvenlik Kurulunun kurulması ve Ulusal Siber Güvenlik Strateji Belgesi ve Eylem Planı bu alandaki önemli köşe taşlarından. Söz konusu metin ve stratejilerin yanı sıra, kritik bilgi sistemi altyapılarının güvenlik yönetimleri, bilgisayar olaylarına müdahale kabiliyetinin arttırılması ve saldırıya uğrayan sistemleri eski işlevine hızlıca geri döndürecek esnekliğin kazandırılması, öncelik verilmesi gereken konular arasında.

Son tahlilde, siber uzay beşinci savaş alanı olarak tanımlanan, hiyerarşi modellerini altüst ederek "tek", "iki" ya da "çok" kutuplu güç dengeleri yerine "farklı" kutuplu (hetero-polar) bir güç dengesi oluşturan, devletler ile bireyler arasındaki kamu gücü ve üstünlüğü kavramını zayıflatarak asimetrik güç ve zafiyet ilişkisi kuran bir dünya. Öte yandan *kritik altyapı sistemlerine* düzenlenen saldırılar aracılığıyla baraj ya da enerji transfer sistemlerinin devre dışı bırakılması, hastane kayıtlarının değiştirilmesi veya finans sistemlerinin çökertilmesi sonucu ciddi zararların ortaya çıkma riski artık sanal değil reel. Bu açıdan aktif ve pasif yönleriyle siber savunma kapasitesinin artırılması son derece önemli. ■