Siber Savaşlar

İNSAMER yuvarlak masa toplantılarında değişen savaş taktiklerinden en can alıcısı olan ve yakın gelecekte güvenlik anlamında tüm dünya devletlerini en çok ilgilendirmesi beklenen siber savaşlar ele alındı. Konuyu Bilişim Güvenliği Uzmanı Onur Yılmaz'dan dinledik. Yılmaz, bilişim alanındaki tecrübeleri ışığında hazırladığı sunumu ile siber savaşları, kişisel güvenlik ve ulusal güvenlik nezdindeki konuları anlattı.

Günümüz dünyası, ilerleyen teknolojiler akabinde internet ve iletişim sistemlerine gitgide daha bağımlı hale gelmektedir. Dünya üzerindeki neredeyse tüm organizasyonlar ve devletlerin tamamınca kullanılan bu teknolojiler, avantajları yanı sıra dezavantajlarını da beraberinde getirmektedir. Gelişen teknolojiler neticesinde, insan hayatının her alanına hızlı ve sınırsız erişimin kendi içerisinde doğurduğu güvenlik açığı, yeni bir savaş tanımı olarak siber savaş kavramını vücuda getirmiştir. Teknik tanımı itibarıyla siber savaş, bilgisayar sistemlerinin farklı amaçlar doğrultusunda ele geçirilmesi, devre dışı bırakılması veya farklı yayınlar yapacak hale getirilmesi işidir.

Bahsi geçen kavram kendisini ticari itibar zedeleme, ego tatmini, ekonomik çıkar gütme, siyasi üstünlük sağlama, espiyonaj ya da bir diğer adıyla casusluk gibi faaliyetlerde göstermektedir. Hem ekonomik hem de fiziksel ve psikolojik anlamda yıkımlara neden olan siber savaşlar üzerindeki yaptırımın sınırları, uluslararası hukukta halen daha net olarak çizilememiştir. Buna büyük ölçüde uluslararası anlaşmalarda yer alan savaşın "silahlı bir faaliyet olduğu" şeklindeki tanımı sebebiyet vermektedir.

Değişen dünya değerleri arasında yerini alarak insan hayatına dâhil olan internet kavramı, kendi içinde hacker adlı yeni bir dil türetmiştir. Elektronik yahut mekanik her sisteme yetkisi olmadan erişebilme kabiliyetine vakıf olanlar şeklinde tanımlayabileceğimiz hackerlar, kimi zaman tekil bir internet kullanıcısını hedef alabilirken, kimi zaman da devletlerin önemli kurum ve kuruluşları ile ticari şirketleri hedef alabilmektedirler. Bilginin kimsenin tekelinde olmadığı inancı ile ortaya çıkan hacktivizm, 1990'lı yıllarda daha çok kişisel menfaatlerle kullanılmış olsa da, günümüzde ulusal güvenlik bazında kullanılmaya başlanmıştır.

Türkiye'de internetin hayatımıza kattıklarının bir getirisi olarak hacker kimlikleri kendilerini daha çok sivil gruplar halinde göstermektedir. Cyber Warrior, diğer bir adıyla Akıncılar grubu da bunlardan bir tanesidir. Bu grup daha çok Mavi Marmara olayı esnasında İsrail sitelerine yaptığı siber saldırılarla bilinmektedir. Ahlaka ve millî değerlere aykırı tüm web portallarını da kendileri için hedef olarak belirleyen Cyber Warrior üyeleri, kendilerini İslam mefkûresi altında savaşan kişiler olarak nitelendirmektedir.

Savaşların gelişen internet teknolojisiyle farklılaşan doğasının vücuda getirdiği siber tehditlerin yüzlerce farklı yöntemi vardır. Kabaca, web sistemlerine yapılan saldırılar, ağ sistemlerine yapılan saldırılar, bilgisayar ve sunuculara yapılan saldırılar ve SCADA (Danışmalı Kontrol ve Veri Toplama Sistemi) gibi endüstriyel sistemlere yapılan saldırılar olarak tanımlayabileceğimiz bu yöntemler, modern insanın kişisel güvenliği ile devletlerin ulusal güvenlikleri açısından büyük tehlikeler arz etmektedir.

Türkiye, resmî kanallarının hedef alındığı bu tarz bir siber saldırıya, son olarak 2015 yılında DDOS diye adlandırılan, sisteme sürekli istek gönderilerek sistemin geçici olarak servis dışı bırakılmasıyla uğramıştır. Resmî kanallardan herhangi bir açıklama gelmese de bu saldırıların Rusya tarafından malum uçak krizi sonrası ekonomik ve resmî işlerde kaos yaratmak için yapıldığı düşünülmektedir. Saldırı en ilkel yöntem olan sisteminin fişinin çekilmesiyle önlenebilmiştir. Çünkü binlerce farklı zombi veya köle olarak adlandırılan sunucudan gelen devasa ölçekteki DDOS saldırılarını yüzde yüz engelleyecek bir koruma günümüzde tam anlamıyla mevcut değildir.

Siber saldırılar, teknolojilerin ulaştığı imkânlar göz önüne alındığında yalnızca devletler bazında değil kişisel bazda da güvenlik tedbirlerini gerekli kılmaktadır. Tekil kişilerce kullanılan teknolojik sistemler; anti-virüsler, güvenlik duvarları ve güncellemelerle daha korunaklı hale getirilebilmektedir. Sanal ortamlarda kullanılan şifrelerin hepsinin farklı olması ve mümkün olduğunca karmaşık şifrelerin tercih edilmesi, uğranacak herhangi bir saldırı riskini en aza indirmeye yardımcı olacaktır.

Bilgisayar, internet ve cep telefonlarının yaygın kullanımı ile bilişim sistemlerindeki hızlı gelişme,

gelecekteki tüm çatışmaların uzayda olacağı tezini destekler nitelikte kanıtlar barındırmaktadır. Tüm dünya devletlerinin siber ordu kavramıyla yeni bir boyuta taşıdığı bu savaş taktiğinin daha nerelere evrilebileceğini ise bizlere zaman gösterecektir.