GÜVENLİK

Siber Güç Kapasitesi Asimetrik Savaşın Parametreleri



Siber ordular, konvansiyonel askerî kapasite bakımından zayıf olan İran, Kuzey Kore ve Suriye gibi ülkeler açısından ilgi çekici bir alternatif. Zira maliyet ve sonuç kıyaslandığında saldırgan lehine olağanüstü bir asimetriden söz etmek mümkün.

Oğuz Kaan PEHLİVAN



Dünya genelinde savaşlar konvansiyonel yöntemlerin çok ötesinde boyutlara ulaşıyor.

Kimi saldırılar ise hava, kara, deniz ve uzaydan sonra savaşın beşinci cephesi olarak tanımlanan siber uzaya taşınıyor. Bu durum siber saldırıları ve maliyetlerini inceleyip uygun stratejiler geliştirmeyi gerekli kılıyor.

Siber savaş ve siber saldırı, sınırları hayli tartışmalı ve yeni kavramlar; bu konularda bir sınıflandırma yapabilmek ya da net tanımlar ortaya koyabilmek için henüz erken bir aşamada bulunuyoruz. Ancak en azından siber saldırının türü bakımından "kim tarafından ve hangi motivasyona" göre gerçekleştirildiğine bakılarak vandalizm ve holiganizmden siber savaşa hatta siber terörizme kadar uzanan bir yelpazede sınıflandırma yapmak mümkün. Ünlü bilgi güvenliği uzmanı Bruce Schneier'a göre, bir siber saldırının siber savaş boyutunda değerlendirilebilmesi için ortada gerçek bir savaş olması gerek. Bu anlamda 2011 yılında Rusya-Gürcistan savaşında Gürcistan'a karşı yürütülen siber saldırılar, siber savaş kapsamında değerlendiriliyor. Yani saldırının "nasıl" yapıldığı aslında onun "ne" olduğunu da belirliyor.

Örneğin; bir devletin elektrik, ulaşım, haberleşme, finans ve su gibi temel kritik altyapılarını işlevsiz hâle getiren siber saldırılar, siber savaş olarak değerlendiriliyor. Tahmin edileceği gibi, bu tarz saldırılar çok ufak maliyetlerle büyük etkiler yaratma kapasitesine sahip. Zaten "az maliyetli bilgisayar teknolojisiyle verilebilecek bir zarar için neden yüksek maliyetli bir füze kullanalım!" fikri, siber savaşın temel motivasyonu. ABD'de "dijital Pearl Harbor" olarak tartışılan böylesi bir saldırının savaş nedeni sayılacağı ve bunu yapan düşmana siber ve kinetik her türlü araçla karşılık verileceği belirtiliyor.

Karşılık verme mevzuunda dikkat çeken diğer bir husus ise BM Şartı ile belirlenen kuvvet kullanımı yetkisine ilişkin. BM Şartı, kuvvet kullanımını sınırlandırıyor ve ancak Güvenlik Konseyi kararı ile meşru müdafaa başlığı altında kuvvet kullanımına izin veriyor. Fakat BM Şartı, siber uzayda kuvvet kullanımı konusunda yetersiz durumda. Siber alandaki hangi saldırılar kuvvet kullanımı olarak algılanacak sorusuna BM henüz cevap veremiyor. Bir haber sitesi ya da hava kontrol sisteminin *hacklenmesi* ya da su arıtma ve kontrol sistemlerine, enerji nakil hatlarının bağlı olduğu sistemlere yönelik saldırılara nasıl karşılık verileceği konusunda ciddi angajman boşlukları söz konusu.

Siber güç projeksiyonları

Suriye iç savaşı bağlamında da saldırıların siber uzaya taşındığına tanıklık ediyoruz. İlk olarak Eylül 2011'de Harvard Üniversitesi'nin resmî web sitesine düzenlediği siber saldırıyla adını duyuran Suriye Elektronik Ordusu (SEA), geçen zaman diliminde faaliyetlerini yoğunlaştırdı. SEA *CNN, Washington Post, Time, NY Times ve Huffington Post* gibi ünlü haber sitelerinin yanı sıra, Türkiye'den de bazı devlet dairelerinin veri tabanlarına da sızmış, şifre ve kullanıcı adlarını ele geçirmişti. En etkili saldırısı ise *Associated Press*'in twitter hesabının ele geçirilerek "Beyaz Saray'a düzenlenen saldırıda Obama yaralandı" şeklinde bir tweet ile *S&P 500* borsa endeksine 136,5 milyar dolarlık zarar yaşatmasıdır. Analistler, SEA'nın iktidara gelmeden önce Suriye Bilgisayar Topluluğu'nun (SCS) başkanı olan Beşşar Esed tarafından desteklendiği ve Suriye ulusal internet altyapısını kullandıkları konusunda hemfikir. Sözü geçen operasyonlar da Suriye'nin siber saldırı kapasitesini her geçen gün artırdığına işaret ediyor.

ABD'nin bu saldırılara nasıl bir karşılık vereceğini kestirmek şu an için zor. *Council on Foreign Relations* uzmanlarından Adam Segal, Amerikan siber ordusunun saldırganın yer aldığı ağlara sızarak saldırganı ve saldırıları etkisiz hâle getirilebilecek ölçüde aktif savunma kapasitesine sahip olduğunu dile getiriyor. Nitekim Edward Snowden tarafından sızdırılan ve ABD'nin gizli siber savunma bütçesi ve operasyonlarını ortaya çıkaran belgeler de bu kapasiteyi ispatlar mahiyette. Belgelere göre, gizli bütçesi 52,6 milyar dolar olan ABD istihbarat servisleri 2011 yılında Rusya, Çin, İran ve Kuzey Kore'yi hedef alan 231 adet "siber taarruz" gerçekleştirdi.

Siber güç kapasitesi aktif ve pasif yönleriyle analiz edildiğinde ABD, Rusya ve İngiltere birinci, Çin ikinci, İran ve Kuzey Kore ise üçüncü kademe ülkeler olarak belirtiliyor. Siber ordular, konvansiyonel askerî kapasite bakımından zayıf olan İran, Kuzey Kore ve Suriye gibi ülkeler açısından ilgi çekici bir alternatif. Zira maliyet ve sonuç kıyaslandığında saldırgan lehine olağanüstü bir asimetriden söz etmek mümkün. Örneğin, 2012'de İran tarafından Suudi enerji firması *Aramco*'nun bilgisayar ağlarının ele geçirildiği ve 300 bin bilgisayarın kayıtlarının silindiği belirtiliyor. Yine, farklı zamanlarda gerçekleştirilen ve pek çok Amerikan bankası ve petrol, gaz ve elektik firmasını hedef alan siber saldırıların arkasında İran'ın bulunduğu sır değil.

Siber saldırıların ekonomik ve siyasi boyutları

Siber saldırıların etkilerini belirlemek ve geniş çaplı bir zarar raporu oluşturmaksa hayli kompleks bir analiz gerektiriyor. Saldırı sonrasında ele geçirilen varlıkların fikrî mülkiyet değeri, sisteme verilen hem donanım hem yazılım zararı, güvenlik sistemlerinin tekrardan kurulum maliyeti gibi pek çok masraf kaleminin dikkate alınması gerekiyor. İşi asıl zorlaştıran ise doğrudan verilen zarardan ziyade yan etki olarak ortaya çıkan sonuçların hesaplanması. Örneğin; bir bankanın bilgisayar ağlarının etkisiz hâle getirilmesi dolayısıyla o bankayla bağlantılı pek çok hizmet aksıyor, bu da zararı kat be kat artırıyor.

Siber güvenlik şirketi *McAfee* ve Washington merkezli *Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS)* tarafından hazırlanan ve Temmuz ayının sonlarına doğru yayınlanan bir rapor, siber suçlar ve siber casusluk faaliyetlerinin ekonomik sonuçlarını ele alıyor. Raporda, finansal varlıkların kaybedilmesinin yanı sıra, fikrî mülkiyet değer-

Siber Suçlar ve Casusluğun Yıllık Maliyeti (56 şirket)

Ülke Analizi	ABD doları
ABD	8.933.510
İngiltere	3.252.912
Avustralya	3.386.201
Almanya	5.950.725
Japonya	5.154.447

Kaynak: Ponemon Institute, *Cost of Cyber Crime Study* Raporu, 2012

leri, marka değerinin ve itibarın zarar görmesi, tüketici kayıpları ve hizmet verilememesi dolayısıyla ortaya çıkan kayıplar değerlendiriliyor. Rapora göre, küresel çaptaki siber aktivitelerin 300 milyar dolar ilâ 1 trilyon dolar arasında değişen oranda zarara yol açma kapasitesi mevcut. Ufak bir kıyas bu rakamları daha anlamlı kılabilir: BM Uyuşturucu ve Suç Ofisi verilerine göre, son derece geniş etki alanına sahip suçlardan olan uyuşturucu ticaretinin küresel ekonomiye verdiği yıllık zarar 600 milyar dolar...

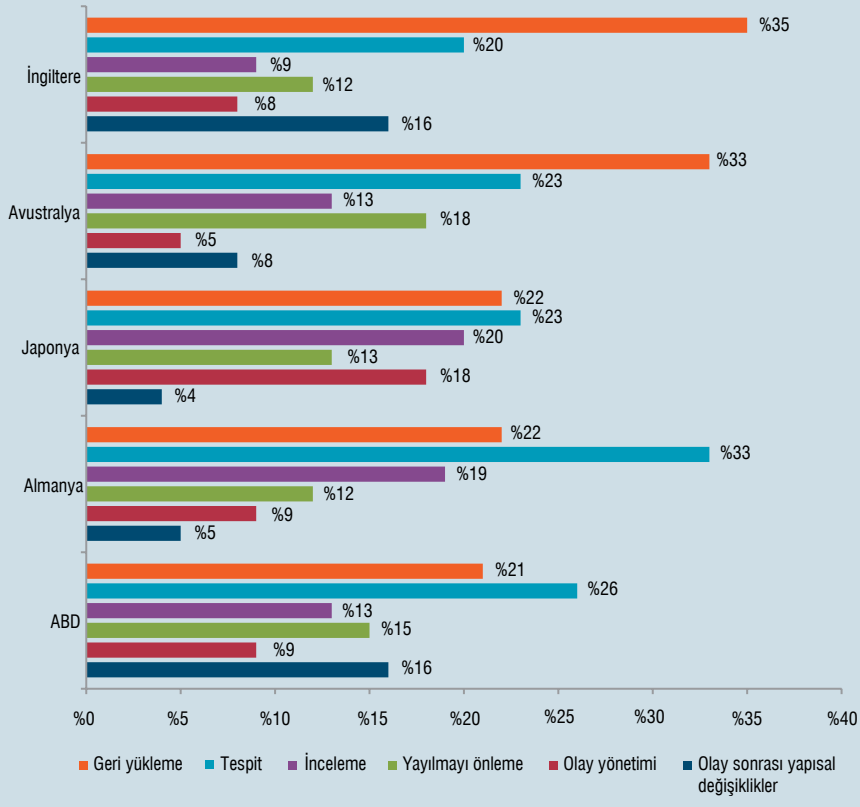
Ekonomik zararların ötesinde dikkate alınması gereken belki de en önemli başlık, siyasi maliyetler. Kritik altyapıları ciddi zarara maruz kalan bir ülkede, birtakım siyasal değişikliklerin de kolaylıkla gerçekleşebileceğini ya da "e-imaj"ı ciddi anlamda zedelenen bir hükümetin, muhaliflerinin eline önemli bir müzakere aracı vermiş olacağını öngörmek zor değil.

Türkiye için stratejiler

Siber tehditleri önleyerek, gelişmiş siber savunma ikaz ve tepki sistemlerine sahip güçlü bir merkezî siber savunma yeteneği kazanmak maksadıyla 2012 yılında Türk Silahlı Kuvvetleri (TSK) Siber Savunma Merkezi Başkanlığı oluşturuldu. Hava Kuvvetleri Komutanlığı'nın sorumluluk sahasına ve fonksiyonel alanına giren siber savunma faaliyetlerinin icra edilmesi ve yönetilmesi amacıyla, bünyesinde Siber Filo Komutanlığı'nın da bulunduğu Siber Komutanlığın kurulması planlanıyordu. Mevcut şartlar dikkate alındığında Türkiye'nin de bir siber harp stratejisi geliştirmesi, siber güç kapasitesini arttırması, siber savunmaya müstakil bir bütçe ayırması ve özellikle Ar-Ge çalışmalarına yoğunluk vermesi gerekiyor. Ayrıca siber güç kapasitesinin projeksiyonunu sağlamak amacıyla siber harp tatbikatları düzenlenmesi de üzerinde durulması gereken bir başka husus. Konunun ekonomik ve siyasal boyutlarının yanı sıra, uluslararası hukuk ve savaş hukuku boyutlarıyla ele alınarak alternatif senaryolar hazırlanması ise elzem.

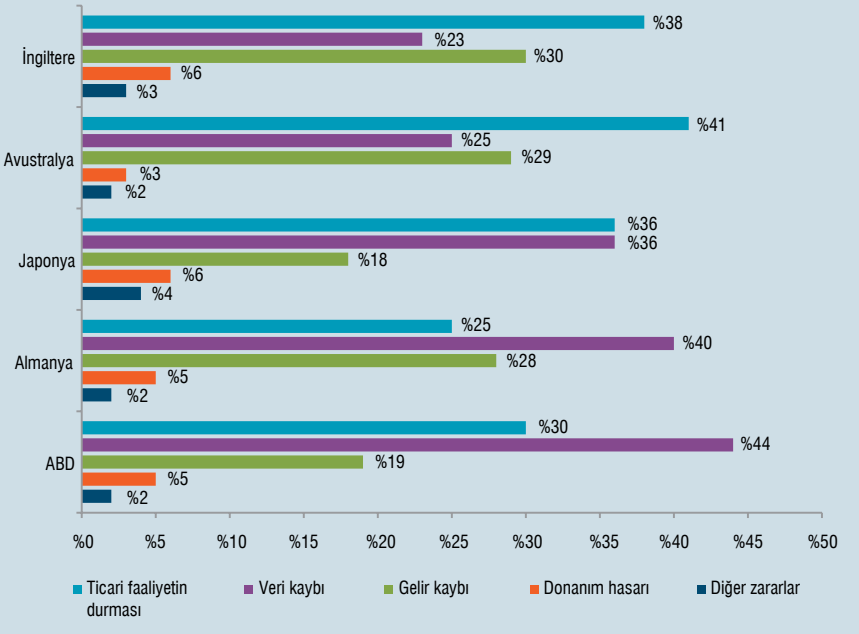
Kısacası, klasik dönemde yalnızca toprakları özelinde egemenlik mücadelesi veren devletler, önce modern dönemle birlikte karasuları, hava sahası hatta uzay sahası üzerinde söz hakkı elde etmeye başladı. Son aşama ise egemenlik haklarının siber uzayda kullanılması olacak. Bu gerçeği dikkate alarak harekete geçmeyen ülkeler açısından büyük zararların söz konusu olacağı bir düzene geçilirken geride kalmamak gerek… ■

Ülkelere Göre Siber Suçun Beş Dahili Maliyet Kalemi



Kaynak: Ponemon Institute, *Cost of Cyber Crime Study* Raporu, 2012

Ülkelere Göre Siber Suçun Beş Harici Maliyet Kalemi



Kaynak: Ponemon Institute, *Cost of Cyber Crime Study* Raporu, 2012