thinktech
STM Teknolojik Düşünce Merkezi

Askeri Siber Gücün Ölçülmesi Neden Önemli?

Herhangi bir yönetim eğitimi kursuna katılmış olan herkes şu sözü duymuştur: "Ölçemiyorsan, yönetemezsin de." Savunma ve güvenlikteki en önemli alanlardan birine dönüşen siber güç söz konusu olunca bilgi ve dolayısıyla bilgiyi ölçmek her şeyden daha önemli hale geliyor. Uluslararası Stratejik Araştırmalar Enstitüsü (IISS) tarafından yayınlanan, Uluslararası Stratejik Çalışmalar Enstitüsü Kıdemli Danışmanı Nigel Inkster imzalı "Askeri Siber Gücü Ölçmek" başlıklı rapor[1] tam da bu konunun önemine işaret ediyor.

Nigel şöyle diyor: "Bugünün ulus devletleri, geçmişin imparatorlukları gibi kendi dönemlerinde rakiplerinin ve düşmanlarının gücünü, potansiyelini iyi kavramış olmayı devletin geleceği için hayati bir araç olarak görür. Devletler askeri kabiliyetlerini gizli tutmayı ister ve tüm yeteneklerinden diğerlerinin haberi olsun istemez. Ancak yakın geçmişteki -özellikle soğuk savaş döneminde- tekniklerin karşılıklı farkındalığı, stratejik bir caydırıcılık kültürüne dönüşmüştür. Devletler tehdit gördüğü diğer ülkelere askeri cepheler açmak yerine caydırıcı başka yollarla bu savaşı sürdürmeyi tercih edebiliyor. Günümüzde ise bilgi ve iletişim teknolojileri dünyasının evrim geçirmesi, bambaşka karmaşıklıklar doğuruyor. Siber alanda gelişen teknolojilere adapte olmak bir yana, sivil ve askeri unsurların bulunduğu bir alanda siber gücün askeri kullanımının ne olduğu sorusunun yanıtı dahi henüz belirsiz."

Siber gücün kabiliyet alanı genişliyor ama bugün bu yeteneklerin askeri olarak benimsenmesinin erken safhalarındayız. ABD Ulusal Güvenlik Ajansı (NSA) Direktörü ve ABD Siber Komutanlığından Amiral Mike Rogers, "Dünya üzerinde şu an yaşanan çatışmaların hepsinin birer siber boyutu da var" diyor[2].

Siber saldırı kısa tanımı ile bir organizasyonun (devletler, şirketler, gizli örgütler vb.) faaliyetlerini bozmak için bilişim teknolojilerinin kullanılması, askeri ya da stratejik amaçlar için bilgi sistemlerinin kasten saldırıya uğratılması olarak özetlenebilir.

www.computerhope.com sitesine göre ise şu unsurlar siber saldırı kapsamında değerlendiriliyor[3]:

- Hükümet veya askeri web sitelerine gizli bilgilere ulaşmak veya gelecekteki saldırılar için zemin hazırlamak amacıyla yapılan girişimler,
- Haber sitelerine yalan haberleri yaymak ve panik yaratmak için yapılan saldırılar,
- Elektrik, su ve gaz gibi temel hizmetlere yönelik saldırılar ve neden olduğu kesintiler,

1 https://www.iiss.org/publications/survival/2017/survival-global-politics-and-strategy-augustseptember-2017
2 https://www.weforum.org/agenda/2018/03/why-we-need-to-measure-military-cyber-power
3 https://www.computerhope.com/jargon/c/cyberwar.htm

- Mali kurumlara, bankalara, hisse senedi alım satımına yönelik, kesintilere veya yanlış bilgi yayımına neden olan saldırılar,
- İnternete yapılan saldırılar.

Inkster'in kaleme aldığı rapora göre bilgisayar teknolojilerinin her dakika gelişmesiyle dünya çapında saldırıların boyutları ve sonuçları da büyüyor: "Askeri alanda siber saldırılar, sabotajlar gerçekleştirerek bankacılık ve finans sistemleri, enerji, sağlık, haberleşme ve ulaşım altyapıları gibi sürekliliği olan operasyonların bozulmasını hedef alabiliyor. Uluslar (Rusya, ABD, Çin örneklerinde olduğu gibi) stratejik ölçekte savaşları kazanmak için bu alanda da ne gerekiyorsa yapabilir. Ancak tam bu noktada neler yapılabileceği, bu gücün etkilerinin ölçülebilir olması önem kazanıyor."

"Siber Alan Savaşın Gidişatını Değiştirebilecek Bir Etken"

Nigel Inkster, sosyal medyanın, kamuoyunu şekillendirmede bir araç, hatta bir güç olarak da kullanıldığına dikkat çekiyor. "Hükümetler, halk üzerindeki psikolojik etkiyi yönlendirmek için, sosyal medya üzerinde çalışmalar, 'operasyonlar' yapıyor. Son olarak Rusya'nın ABD seçimlerine yönelik dijital müdahalesi gibi 'gri bölge' operasyonları daha sık ve yaygın hale geliyor. Siber alan savaşın gidişatını değiştirebilecek bir etken. NATO bunu 2016 Varşova Zirvesi'nde resmi olarak ele aldı ve siber alanı kendi başına bir savaş alanı ilan etti. Silahlı kuvvetler aslında siber yeteneklerin, olasılıkların farkında ama sınırları tanımlanamayan bu gücün ne kadarını kullanabilirler, bundan tam emin değiller[2]."

Çin kendi Stratejik Destek Gücünü, ABD ise Siber Komutanlığını bu alanlarda özelleşmesi ve kabiliyetlerini geliştirmesi için kurdu. Bu birimler, silahlı kuvvetler içinde farklı örgütsel yaklaşımlarla yönetiliyorlar. Inkster'e göre siber gücün askeri amaçla kullanımında bugüne kadar amaç çoğunlukla kısa süreli taktik avantaj sağlamaktı: "Ancak stratejik düzeyde hükümetler artık siber kabiliyetlerini mevcut askeri kabiliyetlerle birleştirip ortaya yeni bir ulusal güç çıkarmayı amaçlıyor; bu yeni ve gri bölgede birkaç adım daha önde olmaya çalışıyorlar[2]."

Siber Saldırılara Karşı En iyi Savunması Olan Ülkeler

Siber savaşın öneminin artması doğal olarak ülkelerin bu tür saldırılara ne kadar hazır olduğu sorusunu da gündeme getiriyor. ABI Research tarafından 2017 yılında hazırlanan Küresel Siber Güvenlik Endeksi'ne[4] göre dünyadaki siber saldırılara en hazır ülkeler sırasıyla Singapur, ABD, Malezya, Umman ve Estonya. Türkiye ise 0.581 puanla dünya sıralamasında 43'üncü sırada yer alıyor.

Ülkeler	Skor
Singapur	0.925
ABD	0.919
Malezya	0.893
Umman	0.871
Estonya	0.846
Mauritius	0.830
Avustralya	0.824
Gürcistan	0.819
Fransa	0.819
Kanada	0.818
Rusya	0.788

4 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Japonya	0.786
Norveç	0.786
İngiltere	0.783
Kore	0.782
Mısır	0.772
Hollanda	0.760
Finlandiya	0.741
İsveç	0.733
İsviçre	0.727

Tablo: ABI Research, 2017 Küresel Siber Güvenlik Endeksi[4]

30'dan Fazla Hükümet Siber Saldırı Yeteneğine Sahip

Dünya Ekonomik Forumunun sitesinde yayınlanan bir başka analizde de, pratikte ABD, Çin ve Rusya'nın siber gücün ne olduğu ve nasıl uygulanacağı ile ilgili küresel algıyı yönlendiren oyuncular olduğu vurgulanıyor[5].

Analize göre bu ülkelerin siber savunma ve saldırı davranışları diğer büyük oyuncuları da yönlendirecektir. Bu yeni alanda öncü olabilmek için ilk adımları atan ABD, bu anlamda Çin ve Rusya'nın önünde yer alıyor. Bu iki ülke, ABD karşısında siber gücün sınırlarını belirme konusunda geride kaldığını düşünüyor. Çin ise son yıllarda kuantum şifreleme ve yapay zekâ yatırımlarıyla ABD'nin teknolojik alandaki üstünlüğü ile rekabet edebileceğini gösteriyor.

Makalenin yazarı Kaja Ciglic'e göre dünyada 30'dan fazla hükümet, saldırı amaçlı siber yeteneklere sahip olduğunu kabul ediyor[5]. Konvansiyonel silahlardan farklı olarak siber araçlar somut ve elle tutulur değil. Kaynağını izlemek ve tanımlamak zor. Inkster ise bu konuda şöyle diyor: "Bu nedenle aslında dünyada siber kabiliyetleri olan devlet sayısı da söylenenden fazla ya da az olabilir ancak büyük ihtimalle daha fazladır."

5 https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention