MÜLAKAT

Bilgi güçse, enformasyon devrimi toplumun geniş kesimlerinin erişebildiği bilgiyi, dolayısıyla gücü arttırdı. Bugün bireylerin güç pastasından aldıkları pay, geçmişe göre çok daha büyük. Bu durum, devletlerin karşılaştığı/karşılaşacağı problemlerin aynı oranda büyük ve zor olması anlamına da geliyor.

JOSEPH

Joseph NYE: *A handout picture released by the official website of Iranian Supreme Leader Ayatollah Ali Khamenei on February 8, 2014 shows him on stage during a meeting with Iranian air force commanders in Tehran.*



NYE

Mülakat: Reyhan Güner & Oğuz Kaan Pehlivan

ARTIK DÜNYA SİYASETİNDE SADECE DEVLETLER VE "ÇOK ÖNEMLİ" OLARAK TABİR ETTİĞİMİZ AKTÖRLER YOK. AKSİNE, OYUNA BİRÇOK YENİ OYUNCUNUN DÂHİL OLMASIYLA BİRLİKTE, DÜNYA SİYASET SAHNESİ HİÇ OLMADIĞI KADAR KALABALIK.

***The Future of Power* (Gücün Geleceği) isimli kitabınızda iktidarların elinde bulunan gücün giderek başka aktörlere kaydığına ve bunun büyük bir politik değişime neden olduğuna işaret ediyorsunuz. Bu değişimin siber alandaki yansıması nasıl olur?**

Siber alanın, gücün dağılımına etki eden enformasyon devrimine güzel bir örnek olduğunu düşünüyorum. Enformasyon devriminden bahsederken esas olarak 1960'lardan günümüze kadar devam eden süreci kastediyorum. Her geçen gün, silikon çipler üzerine çok daha fazla sayıda transistor (iletken) yerleştirebiliyoruz ve bu şekilde bilgisayarların işlem kapasitelerini sıradışı bir şekilde yükseltmiş oluyoruz. Bu aynı zamanda, bir zamanlar küçük şirketlerin ya da bireylerin erişiminin yüksek maliyetli, hatta imkânsız olduğu bilgisayar teknolojilerinin, artık herkes için ulaşılabilir olduğu anlamına geliyor. Örneğin, bir zamanlar uzak mesafeler arasında ya da dünya üzerinde iki farklı nokta arasında iletişim kurmak çok maliyetliydi; ancak bugün telefonunda *Skype* yüklü olan hemen herkes sıfır maliyetle dünya üzerindeki herhangi bir noktayla iletişime geçebiliyor. Dolayısıyla, bir zamanlar yüksek maliyetli olan ürünlere ve hizmetlere, artık pek çok aktör kolayca erişebiliyor. Bu şu anlama geliyor: Artık dünya siyasetinde sadece devletler ve "çok önemli" olarak tabir ettiğimiz aktörler yok. Aksine, oyuna birçok yeni oyuncunun dâhil olmasıyla birlikte, dünya siyaset sahnesi hiç olmadığı kadar kalabalık bir hâl aldı.

Bu gelişmeyi siber alan bağlamında düşünürsek, bir devlet başka bir devletin altyapılarına siber saldırı düzenleyebileceği gibi; bir terörist grubun, hatta gerekli siber kabiliyetlere sahip tek bir kişinin bile bir başka devletin altyapılarına saldırı düzenleyebileceğini söyleyebiliriz. Bu durumun işaret ettiği gerçek şu: Eskiden yalnızca devletlerin erişebildiği, devletlere özgü olan imkânlara, artık küçük gruplar ve bireyler de erişebiliyor. Çünkü enformasyon devrimi sayesinde siber imkânların ucuzlaması, devletin sahip olduklarıyla bireyin sahip oldukları arasındaki engelleri hızlıca yok ediyor. Kitapta bahsettiğim politik değişimin siber alandaki yansımasını bu şekilde özetlemek mümkün.

Bu politik değişim, yumuşak güç bağlamında mı yoksa sert güç bağlamında mı gerçekleşiyor?

Her iki bağlamda da gerçekleşiyor. Enformasyon, diğerlerini etkilemek ve dikkatlerini çekmek için kullanılıyorsa, bu yumuşak güçtür. Eğer ki bu enformasyon başkaları üzerinde kontrol kurmak ve onlara zarar vermek için kullanılıyorsa, bu sert güçtür. Örneğin; İran'daki nükleer tesislerin santrifüjlerine zarar veren *Stuxnet*, sert güç kullanımıydı.

Siber tehditler ve siber saldırılar ülkelerin güvenlik algılarını nasıl etkiliyor?

Bana göre devletler artık, siber alandaki gelişmeler dolayısıyla güvenlik algılarını değiştirmek zorunda olduklarını fark etmeye başladılar. Örneğin siber, tüm ülkelerin ekonomileri için önemli hâle geldi; çünkü ekonomiye tehdit oluşturabilecek güvenlik sorunları, fiziki bir aktörün herhangi bir şekilde bir sınırı geçmesine gerek kalmadan, uzak mesafelerden ve hızlıca ortaya çıkabiliyor. Geçmişte bir saldırı düzenleneceği zaman, bir uçak ya da tankın fiziki bir sınırı geçmesi gerekiyordu. Bugün ise sınırı geçerek gelenler sadece elektronlar. Bu gerçekten alışık olmadığımız bir problem türü. Tüm bunlara ek olarak, söz konusu siber olduğunda *ofansif* (saldırı temelli) hareketler, *defansif* (savunma temelli) hareketlere göre çok daha ucuz ve kolay. Dolayısıyla, siber saldırılara karşı savunma geliştirmek giderek zorlaşıyor. Bu gelişmeler, yeni bir teknoloji dolayısıyla değişen güvenlik algısına örnek olabilir.

Kitabınızdan devam edecek olursak; siber gücün bireylere, ulus devletlere ve yönetişime yansımaları nelerdir?

İlk soruda da değindiğim üzere, enformasyonun ve işlem yapma maliyetinin düşmesiyle birlikte, önceleri sadece devletlere özgü olan birtakım kapasitelere, artık bireyler de erişebiliyor. İnterneti ve uzun mesafeli iletişimi örnek olarak vermiştim. Aynı şekilde uydu görüntüleri, fotoğraflar ve bu kaynaklara erişimden de bahsedilebilir. Uydu görüntülerine erişim, önceleri çok pahalıydı; bu yüzden de yalnızca devletlerin erişebildiği bir teknolojiydi. Ancak şu an insanlar, *Google Earth* kullanarak uydulardan çekilen yeryüzü fotoğraflarına ücretsiz olarak erişebiliyor. İnsanlar böylece daha önce sahip olmadıkları bir kapasiteye de sahip olmuş durumdalar. Eğer ki bilgi güçse, enformasyon devrimi toplumun geniş kesimlerinin erişebildiği bilgiyi, dolayısıyla gücü arttırdı. Bu nedenle bireylerin güç pastasından aldıkları pay geçmişe göre çok daha büyük. Bu durum devletlerin karşılaştığı/karşılaşacağı problemlerin aynı oranda büyük ve zor olması anlamına da geliyor.

Sizce siber güvenlik, geleneksel güvenlik anlayışına ve güvenlik politikalarına karşı çıkıyor mu?

Evet, siber güvenliğin geleneksel güvenlik politikalarına ve anlayışına meydan okuduğunu düşünüyorum. Hepimizin aşina olduğu bir kavram var;

"sınırda savunma". Hatta bu sebeple sınır kontrol mekanizmalarımız, hava savunma sistemlerimiz var. Ancak söz konusu siber olduğunda, sınırda savunma kavramı hiçbir anlam ifade etmiyor. Örneğin Çin gibi ülkeler, çeşitli filtreler vasıtasıyla ülkelerindeki interneti, dünyanın geri kalan internet bağlantılarından izole etmeye çalışıyorlar. Ancak filtrelemenin de yeterli bir çözüm olduğunu söylemek mümkün değil; zira dolaşımdaki bilgi bu filtreleri aşabiliyor. Dolayısıyla problemin ekseninde, insanların internet vasıtasıyla kolaylıkla mobilize olmaları ve bunun yaratacağı bir dizi problem yer alıyor. Sınırda güvenlik kavramıyla başlayan klasik güvenlik politikaları doğruluğunu ve geçerliğini kısmen korusa da bahsedilen şartlar altında yeterli görünmüyor. Bundan yaklaşık 50 yıl önce sınır muhafızları ve hava savunma sistemlerine sahip olmak yeterli oluyordu; fakat günümüzde bu enstrümanlar tek başına yeterli olmuyor.

Biraz da siber istihbarat hakkında konuşalım. Bugün pek çok ülkede siber istihbaratla ilgili negatif gelişmeler söz konusu. Siber istihbarat, insanların güvenliğini mi artırıyor yoksa devletlerin güçlenmesine ve kontrol edilmesi güç araçlara sahip olmasına yol açarak insan güvenliğine tehdit mi oluşturuyor?

Eğer demokratik bir devlet, devasa bir işlem gücü sayesinde kitlesel bir gözetime başvuruyorsa, bu yetki keyfi olarak değil, bu yetkiye birtakım sınırlamalar getiren prosedürlerle birlikte işletilmeli. Örneğin Amerika'daki siber istihbarat tartışmalarının odağında, NSA'nın FISA mahkemesi kararlarına uygun davranıp davranmadığı yer alıyor. Genel olarak NSA, mahkeme kararlarına uygun davrandı; ancak Başkan Obama, hükümetlerin bu gücü bireysel özgürlükler aleyhine kullanmasını önlemek amacıyla, mahkemenin ve denetim mekanizmalarının güçlendirilmesine ihtiyaç olduğuna karar verdi ve bu nedenle bir komisyon oluşturdu. Ayrıca istihbarat örgütlerinin siber gözetimi kötüye kullanmasını önlemek amacıyla kontrol ve denetim mekanizmalarının güçlendirilmesi için pek çok açıklama ve tavsiyede bulundu.

Özetle, gelişmiş bir siber istihbaratın demokratik değerlerin var olduğu ülkelerde insan güvenliği için faydalı olduğu, ancak aksi durumda devletlerin daha da otoriterleşmesine yardımcı olduğu kanısına varabiliriz.

"İnternetin Balkanlaşması" hakkında ne düşünüyorsunuz? Her ülkenin kendi internet yapısını oluşturması, siber alanda düzenlemeler yapması, örneğin internet üzerinde kısıtlama getirmesi siber alanda anarşiye yol açar mı?

Şu ana kadar bir "Balkanlaşma süreci" mevcuttu ama bu kötü bir "Balkanlaşma" değildi. Örneğin, Çin internetteki bazı bilgilere erişimi engellemesine ya da filtrelemesine rağmen, kendisini internetten tamamen koparmadı. Ülkeler her halükârda küresel iletişimin devamını, dolayısıyla internetin devamlılığını sağlayan birtakım iletişim protokollerini kullanmak zorundalar. Bu açıdan daima bir "Balkanlaşma" yaşanacaktır. Fakat korkulması gereken nokta bu değil. Asıl tedirginlik yaratan nokta, "Balkanlaşma"nın bazı ülkelerle iletişimin tamamen kopmasına yol açma ihtimali. Ancak şu an için bu tür bir "Balkanlaşma"dan çok uzağız.

Sizce siber güvenliğe ilişkin genel geçer uluslararası kural ve düzenlemeleri nasıl oluşturabiliriz?

Aslında bu tür kuralların yavaş yavaş geliştiğini gözlemliyoruz. İnternetin kalbini oluşturan bazı konu ve alanlarda, örneğin alan adları (*domain*) sisteminde, internetin uygun bir şekilde çalışabilmesi için hazırlanmış bazı kurallar var. Ancak kişisel mahremiyet ya da içerik kontrolü gibi konularda, üzerinde uzlaşılmış kurallar yok. Fakat devletlerin zaman içerisinde birtakım kurallar geliştirmeye çalıştığı ve bu amaçla bir araya geldiği karşılıklı ve çok taraflı toplantılar mevcut.

Son olarak, siber alanda bizleri nasıl bir geleceğin beklediğine değinebilir misiniz?

Siber, pozitif yönde büyük fırsatlar barındırıyor. Afrika'da pek çok insan, hatta düşük gelirli çiftçiler bile banka işlemlerini cep telefonlarıyla yapıyor ya da mahsulleri hakkında pek çok bilgiye cep telefonları sayesinde ulaşıyor. Dolayısıyla insanlara yeni fırsatlar sunması ve kendilerini geliştirmelerine yardımcı olması noktasında, siber çok önemli bir araç.

Negatif yönü ise siberin yarattığı zayıflıkların ve açıkların, suçluların hırsızlık gibi amaçlarla kötüye kullanabilmesine fırsat sunması. Bu giderek büyüyen bir tehdit.

İnsan doğası gibi, siberin de iyi ve kötü yanları mevcut. Ben iyi tarafın kötü tarafa üstünlük sağlayacağına inanıyorum. Fakat bu üstünlüğün sağlanması ancak, siber güvenliği sağlamak için atmamız gereken adımlar konusunda dikkatli olmamızla sağlanabilir. ■

GELİŞMİŞ BİR SİBER İSTİHBARAT, DEMOKRATİK DEĞERLERİN VAR OLDUĞU ÜLKELERDE İNSAN GÜVENLİĞİ İÇİN FAYDALI OLUR; ANCAK AKSİ DURUMDA DEVLETLERİN DAHA DA OTORİTERLEŞMESİNE YARDIMCI OLACAĞI AÇIK.