SİBER GÜVENLİĞİ ÇİN EKSENİNDE ANLAMAK

Uluslararası sistemin kara, hava ve deniz üçgeni, siber uzayın her geçen gün daha da yer edindiği yaşamlarımızda ana ekseni de sanal dünyanın hegemonyasına kaydırır durumdadır. Bu nedenle günümüzde ülkelerin sınırları, artık, siber alan ölçeğinde güvenlikleştirilmelidir.

Doç. Dr. Arzu Al

Teknolojik gelişmeler söz konusu olduğunda başat güçlerden biri olan Çin Halk Cumhuriyeti için siber dünya oldukça önem arz eden bir konudur. Yaklaşık 50 yıl kadar kendini dış dünyaya kapatarak ciddi bir teknolojik gelişim kaydedip önemli bir teknolojik altyapı oluşturmuş olan devlet, şimdilerde BM'in mevcut rolünün tanınmasına odaklanmış durumdadır. Bir diğer ifade ile devlet, sanal dünyada mevcut olan tüm kaynaklara, uluslararası sistemdeki tüm aktörlerin erişebileceği bir arenayı desteklemeye başlamış durumdadır. Örneğin, kendi sosyal medya platformları olan Renren, Baidu ya da Sina Weibo ile data güvenliğini yıllarca koruyan Çin, çeşitli kısıtlamalar ya da direkt olarak uygulamaya koyduğu sansür çalışmaları ile de kendi siber egemenliğini yıllarca korumuştur. Ancak bu totaliter tavır BM'in devlet politikalarında yer edinmeye başlaması ile 2020 Ocak'ında, ABD elinde olan sunucuların (Facebook ya da Twitter gibi sosyal medya platformları) ilk aşamada politika yapıcıların erişimine açarak, aşılmaya başlamıştır. Nitekim bu durum, küresel internet sanayisinin de hem dengeli hem de şeffaf bir şekilde yönetilmesine olanak tanımaya yönelik bir adım olarak değerlendirilebilir. Bu anlamda da Çin, BM bünyesinde adaletli bir uluslararası internet kurumunun oluşumunu destekleyerek esasında hem ulusal hem de uluslararası siber güvenlikte öncü olmak istediğini dile getirmeye çalışmaktadır. Bir diğer ifade ile çağın gerekliliklerine ayak uydurmaya başlamıştır.

"Siber eylemlerle ülkedeki kritik altyapı fonksiyonlarının zarara uğratılması, internetin, bilginin ve her türlü sanal dosyanın toplum düzenine, ekonomik gelişim sürecine, bireysel mülkiyet hakkına, askeri kapasitesinin gelişimine zarar vermek amacıyla kullanılması gibi etmenlerdir."

Tarihsel bir perspektifte konuya yaklaşıldığında özellikle milenyumun ilk on yılından sonra, bilişim teknolojileri nezdinde sunulan olanakları kullanmaya başlayarak, yeni teknolojik gelişmelere de her geçen sene daha da bağımlı hale gelen Çin için benimsemeye başladığı BM algısı, teknolojik hegemonyasından tamamen vazgeçtiği anlamına da gelmemektedir. Öyle ki konuya özellikle politik perspektifte yaklaşıldığında, ortak bir bakış açısının dışında, yine de Batılı ülkelerden çeşitli noktalarda ayrıştığı görülmektedir. Bakıldığında teknolojik gelişiminin arkasında içe dönük, dışa kapalı bir politikanın benimsendiği yarım asırlık alışkanlıkların hemen geride bırakılması da pek kolay değildir. Çin'de devlet açısından siber güvenliği önemli kılan konular; "siber eylemlerle ülkedeki kritik altyapı fonksiyonlarının zarara uğratılması, internetin, bilginin ve her türlü sanal dos-

1 Doç. Dr. Arzu Al, Marmara Üniversitesi, Siyasal Bilgiler Fakültesi, Uluslararası Politik İktisat Anabilim Dalı Öğretim Üyesi, TESAM Yürütme Kurulu Üyesi.

yanın toplum düzenine, ekonomik gelişim sürecine, bireysel mülkiyet hakkına, askeri kapasitesinin gelişimine zarar vermek amacıyla kullanılması gibi etmenlerdir". Yani aslında bir başka ifade ile yukarıda ifade edilen tehditlere karşı Çin'in uyguladığı politikalar daha ulusal ve uluslararası platforma "kısmen" kapalı olması suretiyle Batılı ülkelerden ayrışmaktadır. Daha bir başka ifade ile de "rakip devletlerin verilerine gizlice ulaşabilmesi, siber casusluk yapabilmesi ve diğer ülkelerin internet tabanlı şirketlerinin altyapısına siber saldırılar düzenleyebilmesi, devletin bu alanda ciddi bir kapasiteye ulaştığını gözler önüne sermektedir". Bakıldığında yürütülen bu politikanın ana yaklaşımı "bağımsız internet teknolojisi olmadan siber güvenliğin sağlanamayacağı yönündedir".

Nitekim 2010 yılında devletin yayınladığı Savunma Raporu'nda da siber alanın özellikle ulusal güvenlik söz konusu olduğunda daha da farklılaştırılarak güçlendirilmesine yönelik, birtakım gerekliliklerin altı çizilmiştir. Bu anlamda belli başlı yatırımların yapılacak olduğunun vurgulanması da önemlidir. Nitekim, Hauke Johannes Gierow 2015 yılındaki çalışmasında, Çin'in uluslararası değil, ulusal güvenliği için siber güvenlik alanında birtakım teknolojik çalışmaları üretmeye devam ederken, aynı zamanda bu alanda küresel aktörlerin hegemonyasından uzaklaşma politikasını da belirli ölçülerde devam ettirdiğini ifade etmeyi unutmamıştır.

Diplomatik açıdan, Çin'in siber diplomasisi üç ana amaç üzerinde hayat bulmaktadır. Bunlar: "Bilişim teknolojilerine yönelik tehditleri sınırlandırmak; siber uzayı ulusal güvenliği temel alarak geliştirerek genişletmek; uluslararası ilişkilerin ana aktörü ABD ve diğer ülkeler başta olmak üzere hem dış hem de iç tehditlere karşı siber güvenlik stratejileri oluşturmaktır". Bu politik yaklaşımlar Çin'in Halk Cumhuriyeti'nce kabul görmüş olan "Siber Güvenlik Kanun"nun ilk maddesinde de oldukça açık bir şekilde karşımıza çıkmaktadır:

"Hukuk kapsamında siber uzay egemenliğini ulusal, sosyal ve kamu menfaatlerini koruyarak, vatandaşların, tüzel kişilerin ve diğer kuruluşların yasal haklarının ve çıkarlarının korunmasıyla birlikte toplumun bilgilendirilmesini sağlayarak gelişimini temin etmek."

Burada özellikle altının çizilmesi gereken bir diğer husus da ekonomik yaklaşımdır. Nitekim bilişim hukuku ve adli bilişim uzmanı Nigar Guliyeva'nın da ifade ettiği gibi

"devletin herhangi bir kurumuna yapılan siber saldırı, ulusal güvenliği krize sokarak devlet kurumlarını ve finans sektörünü etkisiz hala getirebilir; bu tehlikeyi göz önünde bulunduran Pekin, siber güvenlik tedbirlerini gerçekleştirerek ulusal güvenliğini koruma altına almaya çalışmaktadır". Bu nedenle BM nezdinde ortak bir uluslararası siber güvenlik oluşumunu desteklemesinin yanı sıra, öteki taraftan ulusal güvenlik kapasitesinin de gelişimini atlamayan devletin bu duruşu ile rakip ülkelere risk ve tehdit oluşturabilecek kozların da ortaya çıktığı bir gerçektir. Bir diğer ifade ile devletin siber güvenlik konusunda geliştirdiği politikalar güçlü ulusal güvenlik standartlarının oluşturulması dışında, "diğer ülkelerin siber güvenliklerine risk ve tehdit oluşturan bir çizgi" de izlemektedir. Örneğin 2014 yılında Çinli hackerların ABD'ye yönelik çeşitli casusluk faaliyetleri yürüttüklerinin öne sürüldüğü bir kongrede daha sonra Pekin-Washington hattında gerginlik ortaya çıkmıştır. Bakıldığında özellikle altı çizilmelidir ki dünya genelinde yer alan ana sunucuların 13'ünün 10'u ABD tekelinde yer almaktadır. Üstelik bu sunucuların hepsi, "İnternet Tahsisli Sayılar ve İsimler Kurumu"nun kontrolündedir. Bu durum ciddi bir teknolojik gelişme kaydeden Çin için aslında rahatsızlık sebebidir. Bu anlamda içerisinde bulunduğumuz dijital dönüşüm çağında gelecek hamleler de merakla beklenir niteliktedir. Bakıldığında her ne kadar ortak aklın konuşulduğu bir dünya düzeninden bahsediyor olsa da anarşik bir ortam olan siber dünyada, yalnızca devletleri değil, devlet dışı aktörleri de unutmadan, Çin'in daha da ciddi yatırımlar yapacak olduğu beklenmektedir.

"Devletin siber güvenlik konusunda geliştirdiği politikalar güçlü ulusal güvenlik standartlarının oluşturulması dışında, "diğer ülkelerin siber güvenliklerine risk ve tehdit oluşturan bir çizgi" de izlemektedir."

O halde diyebiliriz ki standardı belirleyecek olan dünyayı belirleyecektir...