Cemalettin DEMİRCİOĞLU
Bilgi İşlem Dairesi Başkan Yardımcısı

Siberuzayda Güç ve Güvenlik

İnternet, hiç şüphesiz, günümüz insan yaşamının ayrılmaz bir öğesi haline geldi. Bugün dünyada 3 milyardan fazla insan interneti kullanıyor. 2015 yılına gelindiğinde ise internete bağlı cihaz sayısının insan nüfusunda daha fazla olacağı tahmin ediliyor. Günlük yaşamın ötesinde internetin sosyal, siyasal ve askeri yaşamda bir güç faktörü, ekonomik büyümenin sağlanabilmesi ve sürdürülebilmesi için hayati öneme sahip bir altyapı olduğu da tartışmasız bir gerçek oldu. İnternetin yarattığı bu güç karşısında, son yıllarda, internete bağımlı dünya devletleri, bunların kurdukları organizasyonlar (NATO, AB gibi) ve dolayısı ile Türkiye ciddi bir konsantrasyonla yeni bir güvenlik konseptine yoğunlaştı: Siber Güvenlik.

Birkaç yıl öncesine gidecek olursak 2009 yılında ABD Başkanı Obama (25Mayıs 2009) siber tehditleri ABD'nin karşısındaki en ciddi ekonomik ve ulusal güvenlik sorunu olarak göstermiş, ABD'nin 21. Yüzyıldaki huzur ve refahının siber güvenliğe dayandığını söylemiştir. İngiltere'nin 2010 yılında yayınlanan Ulusal Güvenlik Stratejisinde siber saldırılar, uluslararası terörizm ve uluslararası askeri krizlerle aynı kategoride değerlendirilmiş, stratejinin önsözünde Başbakan Cameron siber saldırıların Britanya'ya ölümcül hasarlar verebileceğini belirtmiştir. 2011 yılındaki NATO Güvenlik Konferansında Alman Başbakanı Merkel (5 Şubat 2011) klasik askeri tehditlerin "geçmişe ait bir şey" olduğunu söyleyerek, NATO'nun yeni stratejik konseptinde herşeyin siber savunma ve siber saldırılar üzerine kurulduğunu ilan etmiştir.

İnternetin popüleritesinin yeni güvenlik tartışmalarının başlamasında katalizör görevi gördüğü bir gerçek ama internetin yeni güvenlik konseptine ismini verebilecek bir güce sahip olmadığı gerçeğini de görebiliyoruz. Çünkü siber güvenlik, siber uzayın sadece bir kısmını (ama önemli bir kısmını) oluşturan internetin güvenliği ile sınırlı değil. O halde siber güvenliği anlayabilmek için siberuzayı ve buradaki güç ilişkilerini de doğru anlayabilmek ilk ele alınması gereken konu olarak karşımızda duruyor. Bu yazımızda daha çok bu konuyu açıklamaya çalışacağız.

Siberuzay

Bugün üzerinde çok şeylerin yazılıp söylendiği siberuzay (cyberspace) tabiri bir bilim kurgu romanı ile insanların karşısına çıktı. Dünyanın en çok okunan bilim kurgu romanlarından biri olan Neuromancer'in (1984) yazarı William Gibson semantik hiçbir karşılığı olmayan bu kelimenin kendisi için bile birdenbire sayfada belirdiğini kendisi ile yapılan bir söyleşide dile getirecektir. Bu etkileyici kelime bugün birçok anlam ifade ediyor. Siberuzay kimilerine göre birbirleri ile haberleşen bilgisayar teknolojileri için kavramsal bir çerçeve, kimilerine göre askeri doktirinde yeni bir cephe, kimilerine göre bütün ekonomik ekosistemin büyüyüp geliştiği bilgiye dayalı bir alt katman, kimilerine göre ise dünya politik arenasında gittikçe önem kazanan yeni bir içerik anlamını taşıyor.

Bir başka açıdan bakıldığında siberuzayın objesel, hibrit bir yapısı da var. Sadece internetle sınırlandırılamayacak bir yapı bu. Standart protokoller kullanarak birbirleri ile haberleşen küresel bilgisayarlar ağını içeren internet, sadece birbirini tanıyan bilgisayarların haberleştiği kapalı intranetler, hücresel teknolojiler (örneğin cep telefonları), fiber optik kablolar, uzay temelli telekominikasyon ve hatta kablolu telefon

→

ağları ve televizyonlar da siber uzayı oluşturan bir bütünün parçaları olarak karşımızda durmaktadır. Buradan bakılınca siberuzayın aslında insan-makine temelli haberleşme araçlarının kullanımı kadar eski bir tarihe dayandığını da söyleyebiliriz.

Siberuzayı sadece fiziksel objelerle açıklamaya çalışmak da onu tam olarak anlamamıza bir engel teşkil edecektir. Siberuzayı anlayabilmek için onun üç katmanını görmemiz gerekiyor (Libicki 2009). İlk olarak, bütün bilgi sistemleri bir kablolar (ve/veya kablosuz ağlar) ve kutulardan oluşan bir fiziksel sistemin üzerine inşa edilir. Fiziksel katmanın (physical layer) olmadığı bir bilgi sisteminden bahsedilemez. Yukarıda bu katmanda neler olduğuna değindik. İkinci katmanda bir makinenin nasıl çalışacağını ve diğer makinelerle nasıl konuşacağını belirleyen sözdizilimsel katman yer alır (syntactic layer) ve biz buna yazılım (software) katmanı da diyebiliriz. Bizim gibi bilgisayar sistemlerini kullanan sıradan insanların anlamlandıramadığı bu katman aslında bütün saldırıların hedefinde olan katmandır. Bilgisayar korsanları makineler üzerinde kendi otoritelerini kurmak için bu katmanı ele geçirmeye çalışır. Son olarak, fiziksel ve yazılım katmanının üzerinde yer alan, bilginin işlendiği ve depolandığı bilgi, anlamsal katman (semantic layer) yer alır. Bu katman bizim için anlamlıdır. Bu bilgileri okuyup, anlamlandırabilir, değerlendirebiliriz. Son olarak şunu da belirtmek gerekir ki, dördüncü bir katman olarak, bilişim sistemlerini kullanan insanı da siberuzayın bir parçası olarak kabul etmek siber güvenliğe doğru yaklaşabilmemiz açısından bir zorunluluk olarak karşımızda duruyor.

Yeni Bir Güç Kullanma Alanı Olarak Siberuzay

Uluslararası ilişkilerde realist bir bakış açısıyla, Nye (2011) bize şu açıklamayı yapar: "Güç istediklerini elde edebilmek için başkalarını etkileme yeteneğidir. Bu yetenek zor güç kullanımı (hard power) ile de yumuşak güç (soft power) ile de gerçekleştirilebilir ve siberuzay bunu gerçekleştirmek için yeni bir alan yaratmıştır. Siber güç siberuzayda kullanılabileceği gibi, siber enstrümanlar siberuzayın dışında da kullanılabilir."

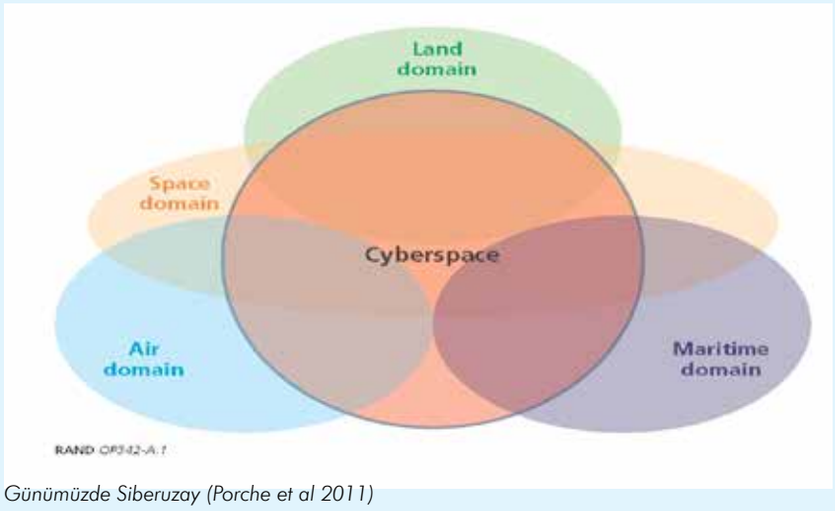
Bir ülkenin bilişim sistemlerini çalışamaz duruma getiren siber saldırılar (Estonya 2007), konvansiyonel bir savaşın etkilerini propaganda ile destekleyecek siber saldırılar (Gürcistan 2008) veya bir fiziksel sistemi çalışamaz duruma getirecek siber saldırılar (Stuxnet, İran 2010) yukarda bahsedilen zor güç ya da yumuşak güç kullanımının birer örneği olarak dünya tarihine şimdiden geçmiş önemli örnekler olarak karşımızda durmaktadır.

Gerçekten de siberuzay birçok uluslararası aktör için (sadece güçlü devletler için değil, küçük devletler, devlet dışı aktörler) yeni birçok fırsatlar yaratmıştır. Nedir bu fırsatlar?

Siberuzay siber aktörlere diğer başka alanlarda olmayan bir imkan sağlar: Kimliğini saklayabilme (anonymity). Siberuzayın kompleks, fiziksel ve sanal mimarisi yetenekli bütün aktörlerin kimliğini ve yerini gizleyebileceği bir matrikse sahiptir. Siber saldırıyı kimin yaptığını ve kime karşılık vereceğinizi çoğu zaman bilemeyebilirsiniz. İkinci olarak şunu rahatlıkla söyleyebiliriz ki siberuzay bütün aktörlere rol alma imkanı bahşetmiştir. Sınırların olmadığı bu aleme girmek herkesin edinebildiği türden internete bağlı bir bilgisayarla dahi mümkün olmuştur. Bu öyle bir kolaylıktır ki isteyen herkes bu aleme girebilir, bu alemde olmak istemeyen de, hatta bu alemde olduğunun farkında olmayanlar da bu alemin bir parçası olmuştur. Siberuzayın sağladığı bir başka garip özellik ise aktörler arasındaki asimetrik güç ve zaafiyet ilişkisidir (asymmetry). Bir bilgisayar korsanı veya bunların bir araya geldiği topluluklar koca devletlere kafa tutabilir, bir güvenlik endişesi yaratabilir. Diğer taraftan örneğin internete bağımlılığın en çok olduğu gelişmiş ülkeler diğer ülkelere nazaran asimetrik bir zaafiyet korkusunu her an hissedebilirler.

Siberuzay aktörler arasındaki güç dengelerini azaltmaya devam etmektedir. Kısacası "yeni uluslararası düzenin tek, çift, çok kutuplu devam edeceğini söylemek zor görünüyor. Yeni dünya düzeni, siberuzayın siber aktörlere sağladığı imkan ve yeteneklerle heteropolar bir yapıya doğru değişmeye başladı (Der Derian ve Finkelstein 2008).

→



Günümüzde Siberuzay (Porche et al 2011)

Daha da önemlisi siberuzay artık Pentagon tarafından kara, deniz, hava ve uzayla birlikte beşinci bir harp meydanı olarak kabul edildi bile (Porche et al 2011).

Kısa Bir Değerlendirme

Okuyucularımızı çok fazla sıkmaması gerektiğini düşünerek kısa bir zamanda yazmaya çalıştığımız bu yazımızın devamında fırsat bulabilirsek siber aktörleri ve bunların kaabiliyetlerini, siber savaş gerçeğini (!), kritik altyapılarımızın korunması için neler yapılabileceğini, Türkiye'nin siber güvenlik stratejisini ve bunun eleştirisini yapmayı düşünüyorum. Ancak yukarıda yazdıklarımızın kısa bir değerlendirmesini sizlerle bazı sorular yardımı ile yapmak istiyorum. Bu değerlendirmeye sondan başlarsak şunları söyleyebiliriz. Kara, deniz ve havada belli bir güce sahip olduğunu düşündüğümüz ülkemiz bunların uzay ve siberuzayla kesiştiği alanlarda ne ölçüde yeterli kaabiliyetlere sahiptir? 20. Yüzyılın ikinci yarısında üzerinde hakimiyet kurulmaya çalışılan uzayda bir varlık gösterebildik mi? 21. Yüzyılda siberuzaydaki yerimizle ilgili ümitli olabilir miyiz?

Siberuzayın güvenliğini ise 4 katmanını yeniden gözden geçirerek düşünelim:

1. Fiziksel katmandaki kablolar ve kutulardan ne kadarına sahibiz? Bunları biz işletebiliyor muyuz? İşletenlerin milli güvenlik kaygıları ne ölçüde var?
2. Bütün tehditlerin hedefindeki yazılım katmanında çözümlerimiz var mı? Kendi işletim sistemlerimiz, güvenlik yazılımlarımız geliştiriliyor mu?
3. Bilgiyi korumak; gizliliğini, bütünlüğünü, erişilebilirliğini sağlamak için yeterli standartlara sahip miyiz?
4. Siberuzayı kullanan ve daha önemlisi siberuzaydaki bilişim sistemlerini yöneten insanlarımız siber güvenliğin ne kadar farkında?

Olması gereken cevapları verebilmemiz için zamanımız giderek kısalıyor. Ancak ümit verici çabaları ve gelişmeleri de yok saymamak gerekiyor. Bunları ilerleyen zamanda birlikte göreceğiz.

KAYNAKLAR

Betz, J.B., Stevens, T. (2011) Cyberspace and the State: Toward a Strategy for Cyber Power, London: The International Institute for Strategic Studies. - Cameron, D. (2011) 'Protecting and Promoting the UK in a Digital World', [Online] Available at: <http://www.cabinetoffice.gov.uk/news/protecting-and-promoting-uk-digital-world > [Accessed 10 February 2012] - Der Derian, J., Finkelstein, J. (2008) 'Cyber Infrastructures and Network Pathologies: The Semiotics and Biopolitics of Heterepolarity', in Dunn Cavelty, M., Kristensen K.S. (eds.), Securing the Homeland: Critical Infrastructure, Risk and (in)Security, Abingdon: Routledge, pp. 84-105. - HM Government (2010) Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, London: The Stationery Office, [Online] Available at: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf?CID=PDF&PLA=furl&CRE=sdsr > [Accessed 10 February 2012] - Jewkes, Y. and Yar, M. (eds.) (2010) Handbook of Internet Crime, Devon: Willan Publishing - Libicki, M. (2009) Cyber Deterrence and Cyberwar, Santa Monica: RAND Corporation, [Online] Available at: <http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf> [Accessed 20 April 2012] - Merkel, A. (2011) 'Speech at Munich Security Conference on 5 February 2011, [Online] Available at: ttp://www.bundeskanzlerin.de/Content/EN/Reden/2011/2011-02-10-bkin-munich-security-conference.html [Accessed 4 May 2012] - Nye, J.S. (2010) Cyber Power, Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs. - Nye, J.S. (2011) 'Power and National Security in Cyberspace', in Lord, K.M. and Sharp, T. (eds.), America's Cyber Future: Security and Prosperity in the Information Age, Volume II, Washington DC: Center for a New American Security, pp. 7-23. - Obama, B. (2009) 'Remarks by the President on Securing our Nation's Cyber Infrastructure', [Online] Available at: <http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure > [Accessed 01 August 2012] - Porche, I.R., Sollinger, J.M., McKay, S. (2011) A Cyberworm that Knows no Boundaries, Santa Monica: RAND Corporation, [Online] Available at: <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.pdf> [Accessed 20 April 2012] - Sommer, P., Brown, I. (2011) Reducing Systemic Cybersecurity Risk, OECD/IFP Project on Future Global Shocks, [Online] Available at: <http://www.oecd.org/dataoecd/57/44/46889922.pdf> [Accessed 10 February 2012] - The White House (2011) International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, Washington: The White House, [Online] Available at: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy _ for_cyberspace.pdf> [Accessed 20 April 2012]