Cemalettin DEMİRCİOĞLU | Bilgi İşlem Dairesi Başkan Yardımcısı

Kurtlar Vadisi Siberuzay (Episode 2): Siber Güçlerin Yükselişi

Geçtiğimiz sayıda dört grupta incelemeye başladığımız siber aktörlerin en güçlülerini, devletleri, bu sayımızda anlatacağımızı belirtmiştik. Siberuzay aktörler arasındaki güç farklılıklarını azaltsa da bu hiçbir zaman bir güç eşitlenmesi anlamına gelmiyordu. Tahmin etmekte sizin de zorlanmayacağınız bazı devletler siberuzayda kendi hakimiyet alanlarını oluşturmakta, yumuşak ve zor gücün bu alanda nasıl kullanıldığını bize göstermektedir.

Yalnız bu konuya geçmeden önce siber güvenlikle ilgili bilgisine ve ülkemize kazandırdıklarına çok değer verdiğim mühendis bir arkadaşımın geçen sayımızdaki makalemizi okuduktan sonra yaptığı önemli bir eleştiriyi sizinle paylaşmak isterim. O makalede haktivistleri politik amaçlarla bir araya gelen hackerler olarak tanımlamış, profesyonel saldırılarla ilgilendiklerini ve çoğu zaman bu saldırıları ve sonuçlarını bir ajitasyon malzemesi yaptıklarını söylemiştik. Doğrusu bazı hususlar eksik kalmış. Arkadaşım der ki: Haktivistler sadece bunlardan ibaret değil. Hatta yukarda söylenenler bir bakıma devletler arası istihbarat savaşlarının sonuçları. Asıl haktivistler genellikle hükümetleri protesto etmek amacıyla sosyal medyada binlercesi gönüllü bir araya gelen ve çoğunun teknik bilgisi kısıtlı olduğu için hazır araçlar kullanarak saldırılar yapan (yaşlı teyzem bile olabilir) kişilerden oluşuyor. Türkiye'deki örneklere bakarsak haktivistlerce kamuya ait yüzlerce web sitesinin taranarak, basit şifrelerin tahmin edilmesiyle yapılan birçok hacking vakasına ya da belli bir gün ve saatte aynı siteye giriş yapılmaya çalışılarak internet sitelerinin erişilmez hale gelmesine neden olan saldırılara tanık olduk. Kısacası siz değerli okuyucularımızdan haktivistleri daha geniş bir perspektifle bir kez daha düşünmenizi rica ediyorum.

> **"Görüldüğü gibi bu ülkelerin siberuzayda sahip oldukları güç bir yana, bu gücün istenerek bir saldırı aracı olarak kullanıldığına da şahit oluyoruz. Bu ülkelerin siberuzay denilince akıllarına daha çok saldırı yeteneklerinin artırılması gelmekte."**

Genel olarak bakacak olursak devletlerin siberuzaydaki gücünün kendi coğrafi sınırları içindeki hükümranlığından kaynaklandığını söyleyebiliriz. Bu sınırlar içinde devletler yasal düzenleme yapma yetkisini kullanarak özellikle internet üzerinde ciddi bir hakimiyet kurabilmektedir. Hatta bu hakimiyet bazı durumlarda coğrafi sınırların dışına dahi taşmaktadır. Bu hakimiyet, siber

→

suç ve siber terörün önlenmesinde ve suçluların yakalanarak cezalandırılmasında önemli bir avantaj sağlamakla birlikte kimi zaman bireysel mahremiyetlerin bu baskın güç tarafından çiğnendiği de ayrı bir tartışmanın konusudur. Biz bu konuyu bir kenara bırakıyoruz.

Burada odaklanacağımız husus yoğun insan kaynağı ve ekonomik imkanlarla siber güç haline gelen ve yeni araçlarla siber saldırılar yapabilen devletlerdir. ABD'de yayınlanan bir çalışma gurubu raporuna göre bu güçler: ABD, İngiltere, Fransa, İsrail, Çin ve Rusya'dır. İngiltere ve Fransa'nın siber operasyonları ile ilgili önemli bir bilgiye ulaşılamadığından (en azından bizim tarafımızdan) diğerlerini burada anlatmaya çalışacağım.

Amerika Birleşik Devletleri

ABD siberuzayı saldırının ön planda olduğu bir savaş alanı olarak gördüğünden burada her zaman en tepede olmayı amaçlamıştır. Bir zamanlar ABD Başkanının ulusal güvenlik danışmanlığını yapmış Richard Clarke'a göre ABD siberuzayda rakipsizdir (second to none). Tıpkı kara, deniz ve uzayda yaptığı gibi siberuzayı kullanarak operasyonlar yapmakta, yabancı ülkelerin ağlarına (networks) düzenli aralıklarla yakalanmadan sayısız sızmalar (penetrations) gerçekleştirmektedir. Pentagon'un 2011 yılı için dünya çapında 88 ülkede 7 milyondan fazla cihazla 15.000 ağa (network) sahip olduğu bir başka saptamadır. Belki bundan da önemlisi, ABD, saldırı kapasitesini geliştirmek, potansiyel siber tehditleri caydırmak için kapalı bir ağda yeni siber silahları test etmektedir.

ABD'nin (İsrail'in de içinde olduğu) dünyada en çok konuşulan siber operasyonu 2010 yılı Haziran ayında İran'ın Natanz şehrindeki uranyum zenginleştirme tesisini bir süreliğine de olsa kilitleyen 'Stuxnet' solucanıdır. Dış dünyaya kapalı bir ağa taşınabilir bir bellekle sokulduğu düşünülen Stuxnet, nükleer zenginleştirmeyi sağlayan Siemens santrifüjlerin dönme hızlarını kontrol eden programları bozarak bunların aşırı ısınmasına ve bunun bilgisayar sistemlerinden gözlenememesine neden olmuştur. Böylece santralin çalışmasını bir süreliğine de olsa durdurmayı başarmıştır. Hikayeyi biraz daha zenginleştirirsek: önce Windows üzerinde çalışan ve Siemens santrifüjleri çalıştırılan yazılımlar Almanya'da ele geçirilmiş, ardından Microsoft Windows'un o zamana kadar bilinmeyen 4 tane açıklığı kullanılarak Stuxnet üretilmiş, bu solucan bir internet kafedeki bilgisayar aracılığıyla uranyum zenginleştirme tesisinde çalışan bir personelin taşınabilir belleğine bulaştırılmış ve bu belleğin içerideki bir bilgisayara taşınması ile her şey altüst olmuştur. İşin garibi bu solucanın daha sonra internet vasıtası ile yayılarak içinde ABD'nin de bulunduğu birçok ülkede yarattığı paniktir. Solucanla ilgili bir rapor hazırlayan ünlü güvenlik şirketi Symantec'e göre Stuxnet o zamana kadar yaratılmış en sofistike ve görülmemiş bir yazılımdır. Bugün bu solucanın etkilerinin iyice azaltıldığını belirterek başka bir siber güce geçebiliriz.

Çin

Çin dünyanın herhangi bir yerinde ve herhangi bir zamanda siber saldırı kapasitesine sahip olmayı amaç edindiğinden teknolojik yatırımlarını sürekli olarak artırmaktadır. Çin'in bir siber güç olarak ortaya çıkmasını onun ekonomik ve askeri gücünün artmasından ayırmamak gerekir. Pentagon'a göre, 2009 yılında Çin Özgürlük Ordusu içerisinde bir siber savaş birimi dahi kurulmuştur. Ancak bu tarihi 2003 yılına kadar götüren yorumcular bulunmaktadır. Nitekim Pentagon bu tarihten itibaren Çin'den kaynaklanan siber saldırıları kayıt altına almaya başlamıştır. İngiltere ve Almanya 2006 ve 2007 yıllarında ciddi siber saldırılara maruz kaldığını ilan etmiş, İngiliz İstihbarat Servisi (MI5) başkanı ülkesinin 300'den fazla özel sektör yöneticisine mektup göndererek kendilerini özellikle endüstriyel casusluk konusunda uyarmıştır.

Çin'le ilgili bir başka önemli iddia ise hükümetin dünyanın her yerine siber saldırılar düzenleyen kendi hacker gruplarına verdiği destektir. ABD'ye göre sayısı 30.000 bilgisayar korsanını bulan yaklaşık 250 grup hükümet tarafından finanse edilmektedir. Örneğin 2010 yılı Ocak ayında dünyanın 34 ülkesindeki teknoloji, savunma ve finans sektöründeki çeşitli firmalara yapılan saldırıların arkasında bu gruplar bulunmaktadır. Bugün Çin'in siber kapasitesi Batı'nın en önemli endişelerinden biridir.

Son olarak hepsinden önemlisi Çin'in sahip olduğu kıyaslanamaz siber savunma yeteneğidir. Bunun nedeni ülkenin tüm internet altyapısının dünyanın başka hiçbir yerine benzememesi ve bu altyapının devletin sahip olduğu bir şirket tarafından yönetilmesidir. Bu sayede Çin, birçok siber saldırıyı en başından engelleyebilmektedir. Bunun dışında Çin hükümetinin tavizsiz

→

tutumu ile Microsoft şirketi bu ülkede kullandırdığı işletim sistemlerinin kodlarını paylaşmak zorunda kalmıştır. Çin'deki Microsoft kullanıcıları kendileri için geliştirilmiş yazılımları kullanmaktadır.

Rusya

Tıpkı ABD ve Çin'de olduğu gibi siber güç Rusya'nın saldırı doktrininde bir güç çarpanı olarak kabul edilir. Rusya'ya göre konvansiyonel askeri operasyonlardan önce siber silahlar düşmanın kritik altyapılarını, askeri ve sivil haberleşmesini ortadan kaldırmak için büyük bir öneme sahiptir. Siber güç ayrıca düşmanın sivil nüfusuna yönelik yapılacak olan psikolojik operasyonlar ve propaganda için önemlidir. Bir diğer husus Rusya'nın bu operasyonları yaparken ülkesindeki devlet dışı aktörlerden de yararlanıyor olmasıdır.

2007 yılının Nisan sonlarında ve Mayıs başlarında Estonya devletinin başkanlık, parlamento, bakanlıklar, siyasi partiler, bankalar, büyük şirketler ve haber kuruluşlarına ait bütün internet siteleri haftalarca sürecek birbirini takip eden siber saldırılara maruz kaldı. Estonya hükümetinin anti-Rus politikalarının iki ülke arasında estirdiği soğuk rüzgarlar, ikinci dünya savaşında hayatını kaybeden Rus askerleri anısına dikilen meçhul asker anıtının başkent Tallinn'deki yerinden sökülerek bir mezarlığı götürülmesiyle doruğa ulaşmıştı. Rus bilgisayar korsanlarının böyle bir atmosferde yaptığı haftalarca süren saldırılar Estonya'nın dünya ile olan internet bağlantısının ortadan kaldırmış, ülkede ciddi bir paniğe neden olmuştur. Bugün NATO Siber Savunma Mükemmeliyet Merkezi Tallinn'de bulunmaktadır. Estonya saldırısından bir yıl sonra bu defa Rusya'nın Gürcistan'la yaptığı kısa savaş esnasında yine Rus hackerlar Gürcistan hükümet sitelerini ele geçirmiş ve ciddi şekilde propaganda yapmışlardır.

İsrail

İsrail Ordusunun siber silah kullanımı her dönemde devam etmektedir. İsrail'in yaptığı bütün operasyonlar esnasında karşı tarafın askeri ağlarına da sızılmaya çalışılarak bu operasyonları kolaylaştıracak sonuçlar elde edilmektedir. Örneğin 2007 yılında İsrail Suriye'ye karşı yaptığı hava operasyonu esnasında bu ülkeye yapılan siber saldırılar sonucunda dünyanın en gelişmiş hava savunma sistemlerinden birine sahip Suriye'nin savunma sistemi çalışamaz hale getirilerek İsrail jetlerinin hedeflerine sorunsuz bir şekilde ulaşmasının yolu açılmıştır. Bugün İsrail'in düzenli olarak Filistin'e karşı siber saldırılar düzenlediği de bilinmektedir. Kimi yazarlar tıpkı gerçek yaşamda olduğu gibi İsrail'in Filistinlilere karşı adı konulmamış bir siber savaşı yıllardır sürdürdüğünü delilleri ile birlikte ortaya koyar. Gerçek dünyadaki saldırılarının vahşetiyle kıyaslanması mümkün olmasa da İsrail'in siber operasyonlarının sonuçları ciddi sonuçlar doğurmaktadır.

Bu Yazı İçin Son Söz

Bu yazımızda dünyanın siber güçlerini sıralayıp bunlardan ABD, Çin, Rusya ve İsrail'i kısaca anlatmaya çalıştım. Görüldüğü gibi bu ülkelerin siberuzayda sahip oldukları güç bir yana, bu gücün istenerek bir saldırı aracı olarak kullanıldığına da şahit oluyoruz. Bu ülkelerin siberuzay denilince akıllarına daha çok saldırı yeteneklerinin artırılması gelmekte. Kendi yarattıkları güvensizlik ortamında dünyanın ve özellikle dünya vatandaşlarının siber güvenliğini nasıl sağlayabileceklerini ister istemez merak ediyoruz. Birleşmiş Milletler Güvenlik Konseyi'nin 5 daimi üyesinin dünya güvenliğini ne ölçüde sağladığı hep tartışma konusu. Dikkatinizden kaçmamıştır, aynı aktörlerin yanına bir de İsraili koyduğumuzda gerçek dünyadaki güvensizlik ortamı siberuzaya yine aynı aktörlerle taşınıyor. Bize gelince, ülkemizin ve vatandaşlarımızın siberuzaydaki güvenliğini sağlayacak tedbirleri almak için çok çok daha hızlı hareket etmemiz gerekiyor.

KAYNAKÇA

Betz, J.B., Stevens, T. (2011) Cyberspace and the State: Toward a Strategy for Cyber Power, London: The International Institute for Strategic Studies. / Farwell, P.J. and Rohozinski, R. (2011) 'Stuxnet and the Future of Cyberwar', Survival: Global Politics and Strategy, 53:1, pp. 23-40. / Inkster, N. (2010) 'China in Cyberspace', Survival: Global Politics and Strategy, 52:4, pp. 55-56. / Jordan, T. (2008) Hacking, Cambridge: Polity Press / Klimburg, A. (2011) 'Mobilising Cyber Power', Survival: Global Politics and Strategy, 53:1, pp. 41-60. / Lord, K.M., Sharp, T. (eds.) (2011) America's Cyber Future: Security and Prosperity in the Information Age, Volume I, Washington: Center for a New American Security / Manson, G.P. (2011) 'Cyberwar: The United States and China Prepare for the Next Generation of Conflict', Comparative Strategy, 30:2, pp. 121-133.

McConnell, M. (2011) 'Cyber Insecurities: The 21st Century Threatscape', 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. 27-39. / 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. / Vacca, W.A. (2011) 'Military Culture and Cyber Security', Survival: Global Politics and Strategy, 53:6, pp. 159-176.