Oğuzhan Vıcıl

## Ulusal Savunmada Yeni Cepheler

# Kritik Altyapıların Siber Güvenliği

>>>

*Derin bir iç çekti adam.*
*Dumanı hâlâ üzerinde olan kahvesinden bir yudum aldı ve her zaman yaptığı gibi kahvaltı masasının üzerindeki günlük gazetelere göz gezdirmek için uzandı.*
*Sıkıntılı olduğundan olsa gerek, elini yavaşça geri çekti.*
*Zaten birkaç haftadır pek iştahı da yoktu, yarım dilim ekmek ve küçük bir parça peynirden oluşan kahvaltısı da çoktan bitmişti.*
*Gözü pencerenin önüne konan güvercine takıldı.*
*Nisan ayı olmasına karşın siyasi havanın kasveti sanki dışarıya da yansımış. Koyu gri bulutlar gökyüzünü kaplamış, etraf alabildiğine karanlık...*

Son iki senede neler olmadı ki ülkesinde. Her şey 2014 yılının başında beklenmedik bir şekilde patlak veren siyasal krizin önce sokak çatışmalarına dönüşmesi, ardından hükümetin istifasıyla sonuçlanan süreçle başlamıştı. 2014 yılının Şubat ve Mart aylarında başlayan siber saldırılar ilk olarak kamu kurumları, medya organları ve telekomünikasyon sistemlerini hedef aldı.[1,2] Bununla iletişim kanallarının tıkanması ve hükümetin Kırım'a zamanlı ve yerinde müdahalesinin önüne geçilmesi amaçlanmıştı. Saldırılar kısmen başarılı da oldu. Ardından gerçekleşen referandumla önce Kırım bağımsızlığını kazandı, sonrasında Rusya'ya bağlandı. Rusya, Ukrayna askeri üslerini ele geçirdi, Kırım para birimi rubleye çevrildi.

Bu duruma ABD-AB ekseninin cevabı sert oldu. Rusya G8 toplantısına çağrılmadı. NATO ülkeleri de Rusya ile askeri-sivil ilişkileri askıya aldı. Ukrayna neredeyse toplumsal olarak ikiye bölünmüş durumdaydı, bir yanda Batı yanlısı AB eksenli taraftarlar, diğer yanda Rusya Federasyonu yanlıları. Seçimler sonucu Batı yanlısı hükümet işbaşında olsa da Rusya yanlıları hâlâ vazgeçmiş değildi. İstikrarın sağlanamamış olması ekonomiyi ve ulusal güvenliği tehdit etmekteydi. Tüm bunlara ek olarak kinetik saldırıların yanı sıra siber saldırılar büyük çaplı olarak ilk defa denklemde yer alıyordu. Zaten ulusal siber güvenlikten sorumlu kişi olduğu için, tüm siber olaylara müdahale eden ekibin başındaydı. Biraz sonra da işinin başında olacaktı.

*Peki, Ukrayna'da AB eksenli hükümetin işbaşına geçmesiyle başlayıp 2014 yılının Nisan ayı itibarıyla Kırım'ın kaybedilmesiyle sona eren süreçte, siber dünyada neler yaşanmıştı; hafızasını biraz zorlayarak düşüncelerinin dünyasında gezinmeye devam etti.*

Kırım'daki referandum sırasında Ukrayna hükümetine ait internet siteleri siber saldırı dalgalarına maruz kaldı. Bu saldırıların hepsi "dağıtık hizmet dışı bırakma" (*Distributed Denial of Service-DDoS*) saldırılarıydı. [1]

2008'de Gürcistan Güney Osetya'yı işgal ettikten sonra Rus Silahlı Kuvvetleri'nin müdahalesi ile eş zamanlı olarak Gürcistan internet altyapısı siber saldırıların hedefi oldu. Gürcistan devlet web sitelerine Rus hacker'lar tarafından propaganda amaçlı içerik eklendi. Gürcistan hükümetine ait web siteleri ile Gürcistan Dışişleri Bakanlığı'na ait sitelerde Gürcistan devlet başkanını Hitler ile kıyaslayan görüntüler yayımlandı.[3,4]

Siber saldırıların arkasında suç amaçlı siber korsanlık toplulukları ve hacktivist'ler varmış gibi görünüyor, Rusya'nın olaya dahli resmi olarak ispatlanamıyordu. Köle bilgisayar ağları (botnetler) vasıtasıyla ele geçirilmiş ve internet vasıtasıyla siber suç çeteleri tarafından kontrol edilen, dünyanın çeşitli yerlerine dağılmış milyonlarca bilgisayar siber suç çeteleri tarafından kullanılıyordu. Her ne kadar bu saldırıların kaynağı tam olarak belirlenemese de siber güvenlik şirketleri en azından Doğu Avrupa kaynaklı siber suç botnetlerinin saldırıda kullanıldığını gözlemlemişti.

Siber saldırıların en önemli özelliklerinden biri de anonimliktir. Siber saldırıların geldiği doğrudan kaynak ile saldırının arkasındaki gerçek kaynak hemen hemen her zaman farklıdır. Bu nedenle özellikle kritik altyapıları hedef alan gelişmiş siber saldırıların hangi devlet dışı aktörler veya devletler tarafından finanse edilip organize edildiğinin tespiti neredeyse imkânsızdır.

Buna ek olarak Rus güçleri Kırım ile Ukrayna arasındaki telefon ve internet kablolarına zarar vererek iletişimi büyük oranda engellemiş oluyordu. Ukraynalı siber korsanların buna cevabı gecikmedi. Güçlü siber saldırılar neticesinde Kremlin, Rusya Merkez Bankası ve Rusya Dışişleri Bakanlığı'na ait web siteleri geçici olarak erişime kapatıldı. Gerçi Rus kaynaklar sonrasında bunun Ukrayna krizi ile ilgili olmadığını iddia etmişti.[1]

Rusya ve Ukrayna'daki hacker'ların suç dosyaları hayli kabarıktır. Rusya-Ukrayna arasındaki krizin başlangıcına kadar iki grup arasından kuvvetli bir dayanışma vardı. Ukraynalı hacker'lar siber korsanlık konusunda hayli etkindir. Örneğin ABD'nin önde gelen perakende şirketlerinden Target'ın, 2013 yılı Kasım-Aralık aylarında maruz kaldığı siber saldırılar neticesinde gizli veriler ele geçirilmiş ve 100 milyondan fazla müşterinin kişisel bilgileri çalınmıştır. Bilgi güvenliği firmaları bu siber hırsızlığın arkasında Ukrayna'nın olduğuna dair birtakım kanıtlar olduğunu belirtmiştir.[5]

İlk başlarda Ukrayna da benzer şekilde siber saldırılara karşılık vermeye çalışsa da bu kadar büyük siber saldırılar karşısında çaresiz kalmıştı.

*Tüm bu düşünceler eşliğinde derin bir iç çekti adam. Ne de çok yorulmuştu son iki senede. Kırım'ın kaybedilmesi neyse de, sonrasındaki iç karışıklık ülkeyi iyiden iyiye germişti. 2014 Mayıs'ında ülkedeki Rusya yanlısı gruplar iç karışıklık çıkarmış, birçok yerde sıcak çatışmalar sonunda kontrolü ele geçirmişlerdi. Ordu ve emniyet güçleri bu olayları bastırmakta ve ilgili bölgelerde kontrolü ele geçirmekte yetersiz kalmıştı. Ülke adım adım parçalanmaya doğru gitmekteydi.*

Kırım ve Rusya arasındaki denizaltı fiber optik internet bağlantısı, Kırım Rusya'ya bağlandıktan sonra yarı özel bir Rus şirket tarafından kurulmuştu. Temelinde Rusya'nın, bilgi güvenliği ve stratejik açıdan Kırım ile arasındaki bağlantının Ukrayna üzerinden yönetilmesini istememesi geliyordu. Buna ek olarak Rusya bu adımla siber saldırı gücünü de pekiştirmiş oluyordu. Ukrayna ise kendisine yapılan fiili saldırılara siber alanda cevap vermek için Ağustos ayında denizaltındaki fiber optik internet bağlantısını kinetik müdahale ile devre dışı bıraktı.

Rusya'nın buna cevabı ise oldukça sert oldu. Ekim 2014'te Kırım yakınlarındaki bir Ukrayna askeri üssü Rus hava saldırısı sonucu yok edildi. İşin ilginç yönü ise, Ukrayna'nın radar sistemleri ve hava savunma sistemlerinin devre dışı kalmış olmasıydı. Rusya, fiili saldırı öncesi siber saldırı destekli elektronik harp tekniğini başarıyla uygulamış oluyordu.

>>>

Operasyon öncesi ve sonrası (Kaynak: Reuters)

6 Eylül 2007'de Suriye'deki bir tesis, nükleer silah geliştirdiği iddiasıyla gece yarısı İsrail savaş uçakları tarafından imha edildi. Hava saldırısını Suriye'nin Rusya'dan aldığı hava savunma sistemleri tespit edememiş, Suriye'nin ancak ertesi gün saldırıdan haberi olabilmişti. İsrail savaş uçaklarının radara yakalanmamış olmasıyla ilgili çeşitli iddialar dile getirildi. Bir iddiaya göre saldırı sırasında İsrail'e ait insansız bir hava aracı elektronik sinyal göndererek Suriye radar sistemini devre dışı bırakmıştı.[6]

Siyasi propaganda yapma ve psikolojik etki oluşturma amaçlı hizmet dışı bırakma ve devlete ait web sitelerini ele geçirme saldırıları alışıldık bir durum haline gelmekle beraber, 2014 yılının Kasım ayındaki siber saldırılar farklı bir boyuttaydı. O güne dek tarihindeki en büyük DDoS saldırılarına maruz kalan Ukrayna'da birçok devlet dairesine ve finansal kuruma çevrimiçi erişilemiyordu. Ukrayna havayolu şirketleri çevrimiçi servislerini devre dışı bırakmak durumunda kalmıştı. Bu sürede tüm işlemler elle, acentelerin intraneti vasıtasıyla yapılmıştı. Banka şubelerinin önünde uzun kuyruklar oluşmuştu. Bu saldırıları daha önceki saldırılardan ayıran en önemli özellik, saldırıların sadece yurt dışından değil, ülke içindeki on binlerce bilgisayardan yapılıyor olmasıydı. Bu nedenle yurt dışı kaynaklı IP'ler engellense bile iç kaynaklı saldırıların önüne geçilmesi bir hayli zaman almıştı. Sonradan anlaşılmıştı ki, zararlı bir web sitesine bağlanan kullanıcıların bilgisayarına otomatik olarak casus yazılım yüklenmesi sonucu bilgisayarların kontrolü siber korsanlarca ele geçiriliyor ve o bilgisayarlar botnet ağının parçası oluyordu. Yani Rusya Ukrayna'daki kritik bilgi sistemlerini yine Ukraynalıların bilgisayarlarıyla vuruyordu.

Sonraki süreçte ise durum çok daha ciddi bir hal almıştı. Nasıl olduğu hala belirlenemeyen bir şekilde, kamu ve özel sektör bilişim sistemlerine virüs bulaşması sonucu özellikle adalet, sağlık ve acil yardım hizmetleri ile ulaşım sektörü bir hafta boyunca çalışamaz duruma gelmişti. Kamu hizmetlerinin aksaması, halk üzerinde psikolojik açıdan "yıkım" etkisi yaptı. Hükümete duyulan güven büyük yara aldı, halkın önemli bir bölümü ABD-AB eksenli tutumun faydadan çok zararı olduğuna ve Rusya ile ilişkilerin bir an önce düzeltilmesi gerektiğine inanmaya başlamıştı. Neyse ki siber olaylara müdahale ekipleri ve NATO'nun Acil Müdahale Ekipleri'nin de teknik desteği ile sistemlerdeki zararlı yazılımlar temizlendi ve sistemler faaliyetlerine tekrar geri döndürüldü.

Kritik altyapılar: İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar.[7]

*Aynanın karşısına geçti adam.*
*Alnındaki kırışıklıkların derinliği dikkatini çekti.*
*Saçlarındaki beyazların arttığını fark etti.*
*Kravatını düzeltti. Ceketini eline almıştı ki birden bire bir üşüme geldi ve tekrar anılar dünyasına dalıp gitti...*

2015 yılının başlarıydı. Sert kış şartları ülkeyi etkilediği için ülkedeki Rusya yanlısı grupların etkinlikleri biraz olsun azalmıştı. Sınır boyunca Rusya ile bölgesel çatışmalar devam etse de henüz savaş durumu alınmamıştı. Bunda Ukrayna hükümetinin daveti üzerine NATO'nun önemli sayılabilecek büyüklükteki birliklerini geçici süreyle ülkeye yerleştirmesinin de etkisi olmuştu. Ancak en vurucu darbe tam da bu süreçte gelmişti. Ülkedeki ana doğalgaz boru hatlarında meydana gelen arızalar ve yer yer de patlamalar nedeniyle doğalgaz iletimi kesik kesikti. Bundan elektrik üretim şebekeleri de nasibini almıştı. Enerji sistemlerindeki sıkıntılar nedeniyle kalabalık yerleşim yerlerinde, örneğin Kiev'de doğalgaz ve elektrik sıkıntısı baş göstermişti. Halk şimdi bir de soğuklarla baş etmek durumunda kalmıştı ki kışın ağır geçtiği bir zamanda bu hiç de kolay değildi.

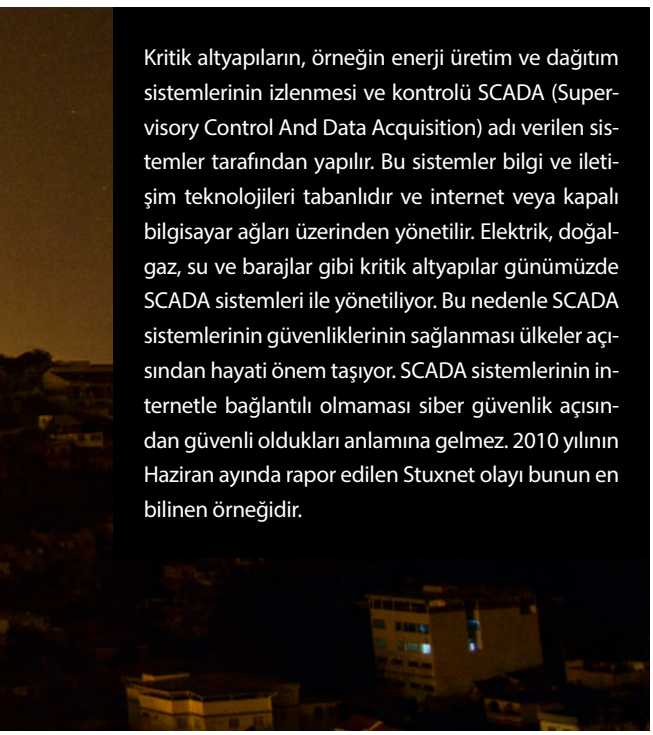
Bu süreçte büyük darbe alan Ukrayna hükümeti konuyu BM gündemine taşımış, sonrasında ise NATO'yu yardıma çağırmıştı. Ukrayna devlet yetkilileri, Rusya ile olan mücadelede NATO ile işbirliğinin gerekli olduğunu ve bir an önce NATO desteğiyle bir siber savunma komutanlığı kurularak tam zamanlı bilgi paylaşımı ve tam harekât kabiliyeti gerektiğini vurgulamıştı. Her ne kadar Rusya Federasyonu bu saldırıların arkasında olmadığını iddia etse de bu denli etkili bir siber saldırının sıradan hacker'lar tarafından değil, arkasında Rusya gibi güçlü bir devlet desteği olan bir organizasyon tarafından yönetilmiş olduğu gerçeği gün gibi ortadaydı. 2015 yazında NATO desteğiyle Ukrayna'da da Siber Savunma Komutanlığı kuruldu ve o günden bu yana yıkıcı etkileri olabilecek siber saldırılar başarıyla savuşturuluyor.

## Stuxnet nedir?

Stuxnet İran'ın nükleer tesislerini hedef alan ve Windows işletim sistemindeki dört adet sıfır-gün açığını kullanan zararlı bir solucan yazılımdır. USB bellek bilgisayara takıldığı anda otomatik olarak sisteme bulaşır ve sistemde hedefindeki bir SCADA sistemi olup olmadığını tarar. Sistem üzerindeki tüm bilgisayarlara bulaşarak hedef SCADA sisteminin kontrolünü ele geçirir. Dünya genelinde yüzbinlerce bilgisayarı etkileyen bu solucan, sadece İran'ın nükleer tesislerindeki SCADA sistemini hedef alacak şekilde tasarlanmıştı. Dış dünyaya kapalı bir ağda yer alan nükleer tesise bulaşan Stuxnet, santrifüjlerin dönme frekansını normalin çok üzerine çıkararak bozulmasına sebep oldu. Bunun neticesinde de İran'ın nükleer programında iki yıllık bir gecikmeye sebep olduğu iddia edildi. Çok karmaşık yapılı bu tür bir yazılımın, çok ileri teknolojiye sahip ülkelerin desteğiyle geliştirilmiş olması gerekir. Bu yazılım geliştirilmesinin arkasında İsrail ve ABD olduğu iddiaları ilgili hükümetler tarafından yalanlanmamıştır.[8]

Stuxnet, siber savaşı sanal ortamdan fiziksel ortama taşımak bakımından çok önemli bir yeri vardır. Dış dünyaya kapalı olan sistemlerin de siber saldırılar neticesinde ele geçirilebileceği ve ulusal güvenlik açısından kritik sistemlerin de hedef alınarak başarılı bir şekilde tahrip edilebileceğini pratikte ispat etmesi bakımından bir kilometre taşıdır.

*Bu düşünceler eşliğinde paltosunu giydi adam, eşiyle vedalaştıktan sonra yavaş yavaş kapıya yöneldi. Siber Savunma Komutanlığı'ndaki işine doğru yola koyuldu...*



Kritik altyapıların, örneğin enerji üretim ve dağıtım sistemlerinin izlenmesi ve kontrolü SCADA (Supervisory Control And Data Acquisition) adı verilen sistemler tarafından yapılır. Bu sistemler bilgi ve iletişim teknolojileri tabanlıdır ve internet veya kapalı bilgisayar ağları üzerinden yönetilir. Elektrik, doğalgaz, su ve barajlar gibi kritik altyapılar günümüzde SCADA sistemleri ile yönetiliyor. Bu nedenle SCADA sistemlerinin güvenliklerinin sağlanması ülkeler açısından hayati önem taşıyor. SCADA sistemlerinin internetle bağlantılı olmaması siber güvenlik açısından güvenli oldukları anlamına gelmez. 2010 yılının Haziran ayında rapor edilen Stuxnet olayı bunun en bilinen örneğidir.

Yazarın Notu: Bu yazıda ulusal güvenliğin siber güvenlik boyutu ele alınmıştır. Siber saldırıların ve siber savaşın kritik altyapılar üzerindeki etkilerinin neler olabileceği, kamu hizmetleri ve toplum psikolojisinin nasıl etkilenebileceği bir senaryo çerçevesinde hikâyeleştirilmiştir. 2014 Mayıs ayına kadar geçen süreçte bahsedilen olayların büyük bir kısmı yaşanmış olaylardan, sonrasında bahsedilen olaylar ise tamamen geleceğe dair senaryo üzerine inşa edilmiştir. Konu edilen senaryoların olabilirliği, geçmişte yaşanan siber olaylara ilişkin referanslar verilerek desteklenmiştir.

**Kaynaklar**
1 "Massive cyberattacks slam official sites in Russia, Ukraine", 18 Mart 2014, www.csmonitor.com
2 http://edition.cnn.com/2014/03/07/opinion/bergen-ukraine-cyber-attacks
3 http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111
4 http://www.nytimes.com/2008/08/13/technology/13cyber.html?em&_r=0
5 "Warner calls for cybersecurity deal with Ukraine" , 24 Mart 2014, http://www.upi.com
6 Cifci, H., *Siber Savaş*, TÜBİTAK Popüler Bilim Kitapları, s. 166-167, 2013.
7 Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı
8 "The Real Story of Stuxnet". *ieee.org*. IEEE Spectrum. 10 Mart 2014.