# Siber Savaşlar

## Bilişimin Karanlık Yüzü

Çinlilerin tarihteki en ünlü başkomutanlarından ve askeri kuramcılarından Sun Tzu günümüzden yaklaşık 2500 yıl önce ünlü başyapıtı *Savaş Sanatı* adlı kitabını yazarken herhalde savaşların bir gün siber savaşlara dönüşeceğini aklının ucundan bile geçirmemiştir. Bilişimin bize armağan ettiği en yeni kavramlardan ve en somut gerçeklerden biri olan siber savaşların, artık klasik savaş olarak adlandırabileceğimiz geleneksel savaşlardan hayli ayrı özellikleri var. Klasik bir savaştakinin aksine bu yeni nesil savaşta düşman binlerce kilometre öteden, hiç beklemediğiniz bir anda -bir görünmezlik zırhına bürünerek- hiçbir kural tanımadan saldırıyor. Bu saldırıların etkisinin fazla yıkıcı olamayacağını düşünen varsa, yanılıyor. Bilgisayarların devletlerin ve toplumların hayatına hemen hemen her alanda girdiği günümüzde iyi planlanmış bir siber saldırının yapacağı etkinin ve yol açacağı yıkımın, en az klasik bir savaşınki kadar yıkıcı ve öldürücü olacağı ne yazık ki bir gerçek. Bilişim çağı ile birlikte artık -aynı nükleer silahlar gibi- yeni nesil bir silah kategorisi doğuyor: Süperbilgisayar virüsleri. Özellikle Ortadoğu ülkelerinde son zamanlarda birbiri ardına ortaya çıkan Stuxnet, Flame ve Mehdi gibi süperbilgisayar virüsleri, internetin giderek artan bir hızla bir savaş meydanına dönüşmeye başladığının kanıtı. Nedir bu süper virüsler, kimler tarafından geliştiriliyorlar, dünyanın hangi ülkeleri virüslere karşı hazırlıklı? NATO'nun yeni siber savaş doktrini ile neredeyse tüm gelişmiş ülkelerde yürürlüğe girmesi için hazırlık yapılan Kill Switch yasası, çıkması olası küresel bir siber savaşı önlemek için yeterli olabilecek mi? Şimdi bu soruların cevaplarını beraber bulmaya çalışalım.

*"Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır"*
*Rex Hughes (NATO Güvenlik Danışmanı)*

### Geleceğin savaş alanı: İnternet

Geleceğin meydan savaşları artık internette yapılacak gibi görünüyor. Çağdaşlaşmanın koşulu olarak bütün devletlerin, şirketlerin ve hatta bireylerin yüksek teknolojili bilgisayar sistemlerine bağımlı hale gelmesi, bu sistemleri aynı zamanda çekici bir hedef haline getiriyor. Esasında bir ülkenin bilgisayar sistemlerinin binlerce kilometre uzaktan bile devre dışı bırakılması hiç de zor değil; bunun için sadece birkaç yüz siber savaşçıya, yeterli donanıma ve internet bağlantısına ihtiyaç var. Haziran 2010'da Stuxnet adlı bir bilgisayar virüsüyle başlayan kâbus, son zamanlarda ortaya çıkan Flame ve Mehdi adlı iki süperbilgisayar virüsü ile hız kazanarak devam ediyor.

Bilgisayar ve internet güvenliğinde uzmanlaşmış, dünyaca ünlü bir firma olan Kaspersky Lab'e göre, küresel ölçekli siber saldırıların sayısı 2011'de toplam 946 milyona ulaşmış. 2010'da meydana gelen toplam 580 milyon siber saldırıyla karşılaştırıldığında bu rakamlar % 61'lik bir artışa işaret ediyor. Uzmanlar, gerek günlük siber saldırıların gerekse Stuxnet, Flame ve Mehdi gibi süperbilgisayar virüsleriyle yapılan saldırıların gelecekte de artarak devam edeceğini tahmin ediyor.

>>>

## Yeni nesil bir silah: Süperbilgisayar virüsleri

Bilgisayarların günlük hayatımıza bu derecede girdiği bir ortamda, devletlerin kendi sınırları içindeki bilgisayar sistemlerini sürekli olarak kontrol altında tutmak, bunun için gereken her türlü önlemi almak zorunda oldukları açık, çünkü düşman artık top, tüfek veya tank ile değil, doğrudan internet üzerinden geliyor. Günümüzde ülkelerin altyapılarının ve savunma sanayilerinin bilgisayar teknolojisine bağlı olduğu düşünülürse, bir savaş sırasında karşı tarafın yapacağı en akıllıca hamle, hedef ülkenin bilgisayar sistemlerini zeki ve kısmen de olsa öğrenme yeteneğine sahip yazılımlar yoluyla ele geçirerek çökertmek.

Aslında bunun ilk örneği 27 Nisan 2007'de Estonya'da yaşanmıştı. Rusya tarafından gerçekleştirildiği tahmin edilen tarihin bu ilk siber saldırısında, Avrupa'nın en gelişmiş bilgisayar ve internet sistemine sahip olan Estonya'da bankalara, devlet kurumlarına, radyo ve televizyon istasyonlarına ait internet sunucuları bir takım siber savaşçılar tarafından birbiri ardına ele geçirilerek haftalarca kontrol altında tutulmuş ve bu saldırının koordine edildiği merkez hiçbir zaman tespit edilememişti. Tam da bu sırada ülkedeki bazı gruplar bir ayaklanmaya kalkışmıştı. İnternet gibi sınırları hayli değişken bir ortamda, siber saldırıların kaynağının tespit ve ispat edilmesi çok zor hatta bazen imkânsız olduğundan, bu saldırının Rusya tarafından yapılıp yapılmadığı hâlâ ispat edilememiştir. Bu olay, Estonya hükümeti tarafından yardıma çağrıldığı halde, gerekli altyapıya ve imkânlara sahip olmadığı için olayı çaresizlik içinde seyretmekten başka bir seçeneği olmayan NATO'ya da bir ders olmuştur. NATO bu tarihten sonra siber saldırılar sorununun üzerine gitmeye başladıysa da, konunun ciddiyetinin tam anlamıyla anlaşılması ve harekete geçilmesi için biraz daha zaman gerekecek ve kurum ancak 2010'da, insanlık tarihinin sabotaj için geliştirilmiş ilk bilgisayar virüsünün ortaya çıkmasıyla içinde bulunduğu rehavetten sıyrılacaktı. Artık hiçbir şey eskisi gibi olamayacaktı.

## Stuxnet'ten Gauss'a

Stuxnet, Duqu, Flame, Mehdi ve Gauss 2010'dan itibaren birbiri ardına ortaya çıkmaya başlayan bu süper virüslerden sadece bir kaçı. Hâlâ deşifre edilememiş ve "görev başında olan" başka süper virüslerin var olması olasılığı da hayli yüksek (bunun en son örneği bu yılın Ağustos ayında ortaya çıkarılan Gauss). Söz konusu süper virüslerin en belirgin özelliği farklı alanlarda "uzmanlaşmış", birkaç işgüzar bilgisayar uzmanı tarafından yazılamayacak kadar karmaşık ve kısmen de olsa öğrenme yeteneğine sahip olmaları. Örneğin Stuxnet sadece önceden belirlenmiş bir konfigürasyona sahip bilgisayarlara ve endüstri sistemlerine zarar vermeyi amaçlarken, Stuxnet'ten sonra deşifre edilen Duqu'nun görevi Stuxnet için yeni hedefler seçmek (dolayısıyla bir nevi keşif virüsü olarak da sınıflandırılabilir). Flame ve Mehdi ise daha çok bilgi sızdırmaya yönelik virüsler. Görevleri içine sızdıkları sistemi tahrip etmekten ziyade kullanıcının e-postalarını okumak, gizli kalması gereken bilgilerini -örneğin şifrelerini- ele geçirmek, ekran görüntülerini almak, bilgisayarın mikrofonunu açarak konuşmaları kaydetmek, daha sonra da kaydettiği tüm bu bilgileri bilgisayarın "arka kapısını" kullanarak, dikkat çekmeden kendi sahiplerine göndermek. Gauss ise yine Kaspersky Lab uzmanları tarafından bu yılın Haziran ayında keşfedildi. Kaspersky uzmanlarından Vitaly

Kamluk'un bildirdiğine göre, Gauss mimarları tarafından tahminen 2011'in Eylül ayında etkinleştirildi, görevi aralarında bu sefer Türkiye'nin de olduğu bazı Ortadoğu ülkelerinde bulunan bankalardaki hesap hareketlerini gözlemlemekti.

Bu süper virüslerin dikkat çekici diğer bir özelliği de dünyanın dört bir yanından ziyade neredeyse sadece İran, Sudan, Lübnan, Suudi Arabistan, Mısır ve Suriye gibi Ortadoğu ülkelerinde ve şu sıralar nadiren de olsa Türkiye'de de etkin olmaları. İnternet güvenliği uzmanı Vitaly Kamluk'a göre bu, siber savaş rüzgârlarının çok yakında bütün Ortadoğu ülkelerinde tüm gücüyle esmeye başlayacağının bir sinyali.

Ayrıca söz konusu süper virüslerde kullanılan yazılım mimarisinden yola çıkan Vitaly Kamluk Stuxnet, Duqu, Flame ve Gauss'un aynı kadrolar tarafından geliştirildiğini düşünüyor. Başka güvenlik uzmanları da aynı görüşte, çünkü her ülkede bu süper virüsleri geliştirebilecek yetenekte çok da fazla bilişim uzmanı yok. İşte bu nedenle, siber güvenlik uzmanları Stuxnet, Flame ve Gauss tipindeki süper virüslerin ancak bir devlet tarafından organize edilen, geniş bir bilişimci kadrosuyla yazılmış olabileceğine dikkat çekiyor.

## İşletim Sistemlerindeki "Arka Kapılar"

Süper virüslerin bilgisayarları bu kadar kolay ele geçirmesinde aslında bilgisayarlarda kullanılan işletim sistemlerindeki birtakım hatalar sonucu açılan "arka kapıların" da payı var. Örneğin Flame'in bilgisayarlara sızmak için, yıllarca Windows'daki bir hatayı kullanıp kendini hedefindeki bilgisayarlara Windows güncellemesi olarak tanıttığı, artık Microsoft tarafından da kabul ediliyor. Microsoft'un –güvenilirliğini yitirmiş bir şifreleme algoritması olarak sınıflandırılmasına rağmen- hâlâ dijital sertifikaların imzalanması için kullandığı MD5 (Message-Digest) algoritmasındaki bir güvenlik açığından yararlanan Flame, bu şekilde kolaylıkla sahte Microsoft imzaları üreterek kendini hedefindeki bilgisayarlara Windows güncellemesi olarak tanıtıyordu. Windows güncellemesi yapmak isteyen hedef bilgisayarı bu şekilde kandıran Flame, söz konusu bilgisayarı esas virüsün bulunduğu bir sunucuya yönlendirerek, kullanıcının Flame'i bilgisayarına kendi eliyle yüklemesini sağlıyordu.

Uzmanların son incelemelerine göre 2007 yılından beri etkin olan ve varlığından ancak programlanmasındaki bir hatadan dolayı bu yıl haberdar olunan Flame, yaklaşık beş yıldan beri Windows'un bu güvenlik açığını kullanarak tüm dünyada yayılıyordu. Her ne kadar söz konusu güvenlik açığının ortaya çıkışından hemen sonra Microsoft tarafından bu açığı kapatacak güncellemeler yayınlanmış olsa da, ne Microsoft'un demode olmuş bu şifreleme algoritmasını hâlâ kullanmasını ne de yıllar boyunca kendi adına dijital imzalar üreten bu virüsün varlığını tespit edememesini anlamak mümkün.

Birleşmiş Milletler'e bağlı Uluslararası Telekomünikasyon Birliği (*International telecommunication Union*, kısaca ITU), Alman Siber Güvenlik yetkilileri (*Bundesamt für Sicherheit in der Informationstechnik*, kısaca BSI) ve güvenlik firmaları Symantec ve Kaspersky tarafından yapılan son araştırmalar, Flame'in başka türde sürümleri de olduğunu, Windows güncellemesiyle yayılan Flame'in artık tanınan sürümünün yanı sıra Windows'daki başka güvenlik açıklarını kullanarak örneğin USB çubukları üzerinden de yayılan başka sürümleri olabileceğini, hatta Flame'den bağımsız başka virüsler de olabileceğini gösteriyor (Kaspersky bir adım daha ileri giderek Eylül 2012 itibarıyla en az üç yeni Flame sürümünün etkin olduğunu iddia ediyor).

Örneğin siber güvenlik firmaları tarafından bu kapsamda Stuxnet üzerinde yapılan analizler sonucu, Stuxnet'in en önemli dosyalarından biri olarak bilinen Resource 207'nin de Windows çekirdeğinde yer alan win32k.sys adlı bir dosyadaki güvenlik açığını kullandığı tespit edildi. (Bu dosya aynı zamanda içerik ve işlevsellik açısından atmpsvcn.ocx adlı Flame dosyası ile neredeyse tıpatıp aynı. Bu bulgu, söz konusu iki virüsün, ayrı ama birbiriyle yardımlaşan iki ekip tarafından geliştirildiğini gösteren önemli kanıtlardan biri. Siber güvenlik uzmanları, bazı ortak mimari ve işlevsel özelliklere sahip olan ve neredeyse sadece Ortadoğu ülkelerinde etkili olan Duqu'nun, Flame'in ve Stuxnet'in ABD ve İsrail tarafından geliştirildiğini iddia ediyor.)

Bütün bu siber savaş boyunca Stuxnet, Flame gibi virüslerin hangi platformlar üzerinden kontrol edildiğine bakınca başka bir gerçekle daha karşılaşıyoruz: Linux! (*bkz.* Ege, B., "UNIX 40 Yaşında", *Bilim ve Teknik*, s. 34-37, Şubat 2012) Elde edilen bilgilere göre Duqu CentOS Linux'un, Flame ise Linux'un diğer türevlerinden Ubuntu Linux veya (64 bitlik) Debi-


lamıştı. Bu kapsamda NATO'nun amaçlarından biri de bir siber savaş doktrini oluşturmaktı. 2010'da Stuxnet'in deşifre olmasıyla birlikte, uzun bir süreden beri siber savaş konusunda suskunluğunu koruyan NATO alarma geçerek doktrin konusundaki çalışmalarına hız verdi ve yeni geliştirdiği siber savaş doktrinini 2011 Haziran'ında açıkladı. Bu doktrine göre, NATO önemli tesisleri, altyapıları ve insan hayatını tehlikeye sokan herhangi bir siber saldırıyı silahlı bir saldırıyla eş tutacağını ve gerekirse bu türdeki siber saldırılara silahla karşılık vermekten kaçınmayacağını açıklıyordu. Bu dünya tarihinde bir ilkti ve savaş tarihinde yeni bir dönem başlıyordu. Artık dünyanın teknolojik yönden en gelişmiş ülkeleri kara, deniz, hava ve uzay kuvvetlerinden sonra beşinci bir kuvvet olarak kendi siber kuvvetlerini resmen kurmaya başlayabilirdi.

### NATO'nun yeni siber savaş doktrini

Yukarıda da belirtildiği gibi 2007'de tarihin ilk gerçek siber saldırısıyla karşılaşan NATO, bu saldırıya hayli hazırlıksız yakalanmış ve saldırı sonrasında bazı hazırlık çalışmalarına baş-

### Yeni nesil bir ordu: Siber ordular

Yine 2011 Haziran'ında ve neredeyse NATO'nun yeni siber savaş doktrinini açıklamasıyla eş zamanlı olarak, Çin 30 siber savaşçıdan oluşan bir siber ordu kurduğunu resmen açıkladı.

>>>

an Linux'un kullanıldığı sunucular üzerinden kontrol ediliyor, daha doğrusu yönlendiriliyor (Kaspersky tarafından açıklandığına göre söz konusu kontrol sunucuları, başta Almanya olmak üzere Hollanda, İngiltere, İsviçre, Hong Kong ve hatta Türkiye'de). Bu sunucularda yer alan kodlar ise ağırlıklı olarak PHP ile geliştirilmiş. Ayrıca Flame'i geliştirenler sızdıkları bilgisayarlardan elde ettikleri ve bu kontrol sunucularına yükledikleri verileri kendilerinden başka hiç kimsenin ulaşamaması için hiçbir çaba ve masraftan kaçınmayarak son derece gelişmiş yöntemlerle şifrelemişler.

Burada okuyucunun aklına, Windows yerine alternatif bir işletim sistemi olarak, örneğin Linux kullanmanın hedefteki bir bilgisayarı dışarıdan gelebilecek tehlikelere karşı koruyup korumayacağı sorusu gelebilir. Aslında bu sorunun cevabı açık: Hayır. Çünkü aynı Windows'taki gibi her Linux sürümünde de ister istemez hatalar oluyor. Hatalar ve dolayısıyla güvenlik açıkları da ancak zamanla ortaya çıkıyor. İşte o arada da işletim sistemine ait bu açıkların kötü niyetli kişiler tarafından tespit edilip bir nevi "arka kapı" olarak kullanılması durumunda bilgisayarınız açık hedef haline geliyor. Bazı çevrelere göre ise işletim sistemlerinin hemen her sürümünde rastladığımız bu güvenlik açıkları, gelecekte "arka kapılar" olarak kullanılmak üzere üreticiler tarafından özellikle bırakılıyor (örneğin son yıllarda ABD'de ve Avrupa ülkelerinde yapılan araştırmalar özellikle Çin'den gelen donanım ve yazılımlarda bu türdeki arka kapılara sıkça rastlandığına işaret ediyor).

Yukarıda yazılanlardan da anlaşılacağı gibi her ne kadar günümüzde teknoloji hayli gelişmiş olsa da en azından insan kaynaklı hatalardan dolayı, ister donanım olsun ister yazılım, hatasız bir bilgisayar sistemi düşünmek mümkün değil. Bu durumun gelecekte de böyle devam edeceği çok açık. Fakat bu gerçek bir yandan artık günlük hayatımıza girmiş olan bilgisayarlara karşı gerçekleştirilebilecek yeni siber saldırılara adeta davetiye çıkarırken diğer yandan da bizlere bir çare kapısı aralıyor ve yeri geldiğinde bu saldırıları düzenleyenlerin de en az "kurbanları" kadar yaralanabilir olabileceğine işaret ediyor. Çünkü bu süper virüsleri yönlendiren tüm kontrol sunucularının bir işletim sistemi ve o işletim sisteminin de en az bir hatası olması gerektiği teknolojik bir gerçek. Dolayısıyla siber savunmanın püf noktası çökmeyecek hiçbir sistem olmadığını bilmek ve kullanmakta olduğunuz sistemdeki olası hataları, diğer bir deyişle "arka kapıları" bulup zamanında kapatmak. Bunu gerçekleştiren bir siber ordu aynı Sun Tzu'nun ordusu gibi yenilmez olacak ve olası bir "siber savaşı" daha başlamadan yarı yarıya kazanmış sayılacaktır.

**Kaynaklar**
RT, "USA and Israel behind Flame virus", **http://rt.com/news/us-israel-flame-iran-251**, 20 Haziran 2012
Kaspersky Lab, "Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected", **http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected**, 11 Haziran 2012
ZDNet, "Kaspersky meldet drei neue Flame-Varianten", **http://www.zdnet.de/88123871/kaspersky-meldet-drei-neue-flame-varianten**, 18 Eylül 2012
Heise Security, "Kaspersky: Stuxnet und Flame sind doch verwandt", **http://www.heise.de/security/meldung/Kaspersky-Stuxnet-und-Flame-sind-doch-verwandt-1615509.html**, 11 Haziran 2012
Microsoft Security Research & Defense, "Microsoft certification authority signing certificates added to the Untrusted Certificate Store", **http://blogs.technet.com/b/srd/archive/2012/06/03/microsoft-certification-authority-signing-certificates-added-to-the-untrusted-certificate-store.aspx**, 03 Haziran 2012
Microsoft Security Research & Defense, "Flame malware collision attack explained", **https://blogs.technet.com/b/srd/archive/2012/06/06/more-information-about-the-digital-certificates-used-to-sign-the-flame-malware.aspx**, 06 Haziran 2012

Bu haberi diğer NATO ülkelerinin (ABD, İngiltere, Almanya ve Türkiye) kendi siber ordularını zaten kurmuş veya kurmak üzere olduğu ile ilgili haberler izledi (şu anda NATO'nun Brüksel'deki ana karargâhında görevi sadece siber savunma olan en az 100 bilişim uzmanı çalışıyor). Günümüzde gerçekleşen "sanal silahlanma" sürecinin, en az gerçek silahlanma süreci kadar ciddi boyutlara ulaşmış olduğunu söylersek abartmış olmayız. Bilgi Güvenliği Derneği Başkanı Prof. Dr. Mustafa Alkan'ın verdiği bilgiye göre, siber saldırılardan korunmak için günde 12 milyon dolar harcayan ABD'nin maruz kaldığı siber saldırılar nedeniyle yıllık toplam ekonomik kaybı 100 milyar doları buluyor.

Siber orduların hangi niteliklere sahip kişilerden oluşması ve kimler tarafından yönetilmesi gerektiği önemli bir soru. Uzmanların bu konudaki görüşleri birbirinden farklı, ancak en yaygın görüş, ABD'de ve Almanya'da da olduğu gibi bir ülkenin emniyet ve istihbarat teşkilatları ile silahlı kuvvetlerinin ortaklaşa çalışması gerektiği yönünde.

## Kill Switch!

İnternete hâkim olan bu belirsizlik ve soğuk savaş ruhu, teknolojik yönden dünyanın en ileri ülkesi konumunda olan ABD'nin bile gözünü korkutmuş olmalı ki, ABD'li Senatör Joe Liebermann önderliğindeki bir grup uzun zamandan beri Kill Switch adı verilen bir yasa tasarısı üzerinde çalışıyor. Yasanın amacı, herhan-

gi bir siber saldırı anında ABD Başkanı'na ülke sınırları içinde interneti tamamen "kapatma" yetkisi vermek. Her ne kadar ABD Başkanı Obama'nın kişi özgürlüklerini kısıtlayabileceği endişesiyle bu yasa tasarısını henüz benimsemediği iddia edilse de, bu durum ABD'nin yakın bir gelecekte uğrayabileceği herhangi bir siber saldırıyla hızla değişebilir. Üstelik bu konuda ABD tek başına değil; ABD ve Avrupa basını, bazı Avrupa Birliği ülkeleri de dâhil olmak üzere başka gelişmiş ülkelerde de benzer bir yasanın çıkarılması yönünde çalışmalar yapılmakta olduğunu iddia ediyor. Böyle bir uygulamanın gerçekçi olup olmadığını ve toplumlar tarafından kabul görüp görmeyeceğini önümüzdeki yıllar gösterecek.

## Einstein 3

ABD'nin siber savaş alanındaki bir diğer gizli silahı da Einstein 3 programı. ABD'nin dünyaca bilinen gizli teknik servisi NSA (*National Security Agency*) tarafından programlanan bu yazılımın amacı, internete ve diğer ağlara sızan kötü niyetli yazılımların otomatik olarak tespit edilerek etkisiz hale getirilmesi.

## Türkiye

Bilgi Güvenliği Derneği Başkanı Prof. Dr. Mustafa Alkan'ın belirttiğine göre Türkiye, siber saldırılara çok yoğun maruz kalan 10 ülkeden biri. Şu anda sadece ABD, Rusya, Çin, İngiltere, İsrail ve İran'ın gerçek anlamda siber orduya sahip olduğunu belirten Prof. Alkan, bu ülkelerin sadece savunma değil saldırı amaçlı siber timlere de sahip olduğunu vurguluyor. Gazi Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı Şeref Sağıroğlu ise Türkiye'nin günde ortalama 15.000 siber tehdide maruz kaldığını belirterek ülkemizin şu anda bile fiilen siber savaş halinde bulunduğunu vurguluyor. İnternet güvenlik şirketlerinden McAfee tarafından 2012 başında açıklanan bir güvenlik araştırması, siber saldırılara en hazırlıklı ülkelerin İsrail, Finlandiya ve İsveç olduğunu ortaya koyuyor. Birçok ülke gibi Türkiye'nin de bu noktada daha çok yol kat etmesi gerektiği açık. Bu nedenle geçen yıl TÜBİTAK ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından ilki gerçekleştirilen Ulusal Siber Güvenlik Tatbikatı'nın ikincisinin bu senenin sonuna doğru yapılması planlanıyor. Geçen yıl kırk bir kuruluşun katılımı ile yapılan tatbikata bu yıl yüzün üzerinde kurum ve kuruluşun davet edilmesi ve tatbikat çerçevesinde bu defa gerçek saldırıların da düzenlenmesi hedefleniyor. Ülkemizde bu tip tatbikatların düzenli aralıklarla yapılması, hem devlet kurumlarının siber saldırılara hazır olması hem de geliştirilen siber savunma yöntemlerinin denenmesi açısından hayli önemli; çünkü siber savunmanın sırrı aynı zamanda siber saldırıda yatıyor ve geliştirilen savunma taktikleri var olan başka sistemler üzerinde denenmedikçe bunların gerçekten etkin yöntemler olup olmadığı anlaşılamıyor.

## Sonuç

Yukarıda da belirtildiği gibi, yakın zamanda geliştirildiği belli olan ve birbiri ardına ortaya çıkan Stuxnet, Flame ve Mehdi gibi yeni nesil süperbilgisayar virüslerinin sadece birtakım işgüzar bilgisayar korsanlarının eseri olmadığı, hatta arkalarında konularında söz sahibi bazı bilişim uzmanları ile gelişmiş devletlerin bulunduğu açık. Yakın bir gelecekte bu tipte siber silahlarla gerçekleştirilebilecek saldırıların, sonuçları açısından klasik savaşları aratmayacağı ortada: Elektrik santrallerinin devre dışı bırakılması, nükleer santrallerin kontrollerinin ele geçirilerek potansiyel birer atom bombasına dönüştürülmesi, basıncın artırılarak doğal gaz boruların havaya uçurulması, baraj kapakları açtırılarak şehirlerin sular altında bırakılması, iletişim ağlarının devre dışı bırakılmasıyla haberleşmenin sekteye uğratılması ve hava, kara ve deniz trafiğinin aksatılması.

İleri teknoloji ve bilgisayar sistemleri, insan yaşamını kolaylaştıran unsurlar olarak devletlerin, toplumların ve bireylerin hayatına her geçen yıl daha fazla giriyor. Bununla doğru orantılı olarak siber tehditlerin sayısı artsa da, bilgisayarlaşmadan vazgeçilemeyeceğine ve birtakım yerel internet ağları kurmak bir ülkeyi dünyadan koparmaktan başka bir işe yaramayacağına göre, siber saldırılar yoluyla gelebilecek tehditlerin önüne geçilebilmesi için üç ana önlem alınması gerekiyor. Bunlardan ilki, NATO Güvenlik Danışmanı Rex Hughes'un da belirttiği üzere, Nükleer Silahların Yayılmasının Önlenmesi Antlaşması (1970) örneğinde olduğu gibi uluslararası savaş hukukunun bir an önce güncellenerek, savunma amaçlı olmayan siber saldırıların kesin olarak yasaklanması. İkincisi ise ülkelerin beşinci kuvvet olarak savunma amaçlı siber ordular kurması. Üçüncü ve belki de en pahalı önlem ise herhangi bir otokontrol mekanizması olmayan ve artık kullanıcıların güvenlik ihtiyaçlarına cevap vermekten uzak olan günümüz internetinin (Web 2.0) bir an önce bilgisayar odaklı internete dönüştürülmeye başlanması (bkz. Ege, B., "Yeni Bilgi Modelleme ve Programlama Felsefesiyle Semantik Web", *Bilim ve Teknik Dergisi*, s.36-39, Aralık 2011).

İngiltere'nin eski başbakanlarından Gordon Brown'unda da belirttiği gibi devletlerin büyük bir güç olabilmek için artık sadece açık denizlere değil, aynı zamanda internete de hâkim olması gerekiyor.


Fotoğraflar: thinkstock

**Kaynaklar**
TÜBİTAK, "2. Ulusal Siber Güvenlik Tatbikatı Hazırlıkları Başladı", 9 Ağustos 2012, **http://www.tubitak.gov.tr/sid/0/pid/0/cid/29120/index.htm**
TÜBİTAK & Bilgi Teknolojileri ve İletişim Kurumu,"Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu", 25-28 Ocak 2011.
Symantec Corporation - Security Response, Falliere, N., O Murchu L., ve Chien E., "W32.Stuxnet Dossier", 4. basım, Şubat 2011.
Nedoklan, M., "Nato Staaten rüsten für das fünfte Schlachtfeld", *Der Spiegel*, 1 Haziran 2012.
Kaspersky Lab, Global Research and Analysis Team, "Gauss: Abnormal Distribution", Ağustos 2012.
Reissmann, O., "Neue Sicherheitsdoktrin: USA erklären das Netz zum Kriegsschauplatz", *Der Spiegel*, 1 Haziran 2011.