

Yeni Dünya'nın Keşfi

Siber Fırsatlar ve Tehditler

Oğuz Kaan PEHLİVAN & Reyhan GÜNER



Fırsatları ve tehditleriyle siber dünya, geleneksel yaklaşımları değişime zorluyor. Sosyo-ekonomik ve politik yapılar üzerinde etkili olduğu gibi siber suçlar, saldırı ve istihbarat yönleriyle fırsatları bir tehdide dönüştürme potansiyelini de içerisinde barındırıyor.

1990'lı yıllarda etkisi iyiden iyiye hissedilmeye başlayan bir değişim dalgasıyla karşılaştık: "Bilgi Devrimi". Bu devrimin temel esprisi, bilgiye erişimi sağlayan araçlarda kökten bir farklılaşma yaşanmasıydı. Nasıl mı? Bilginin dolaşımı matbaanın icadından bu yana -500 küsur yıldır- kâğıt üzerinden gerçekleşiyordu. Ama artık karşımızda kâğıttan çok ekranlar var. İlk önce *bilgiyi depolama* kapasitemiz gelişti, sonraları ise *bilgiyi işleme* ve anında *geri çağırma*. Artık bir memurun veri ya da evrak bulmak için küf kokulu, tozlu arşivlere girmesine gerek kalmadı. İstenen veriyi dijital ortama aktarmak, depolamak, tasnif etmek ve gerektiğinde geri çağırmak günümüzde son derece kolay.

Kişisel bilgisayarların hayatımıza girişi, temel olarak birbirine bağlı bilgisayarlardan oluşan internetin dünya çapında giderek yaygınlaşması, teknolojinin hızlı gelişimi ve bir bilgisayarın sahip olduğu özelliklerin artık cep telefonlarına, hatta beyaz eşyalara uyarlanması, konuyu basit bir devrim olmanın da ötesine taşıdı. Zira gerçek dünyayla iç içe olan siber dünya, çift yönlü kullanımlara sahip: İyi-kötü, fırsatlar-tehditler, açılımlar-kısıtlamalar...

Bu noktada bilgisayarlardan, kullanıcılardan, ağlardan ve yazılımlardan oluşan siber dünyayı, fırsatları ve tehditleriyle beraber mercek altına almak, uygun stratejileri ve politikaları tespit etmek önem arz ediyor.

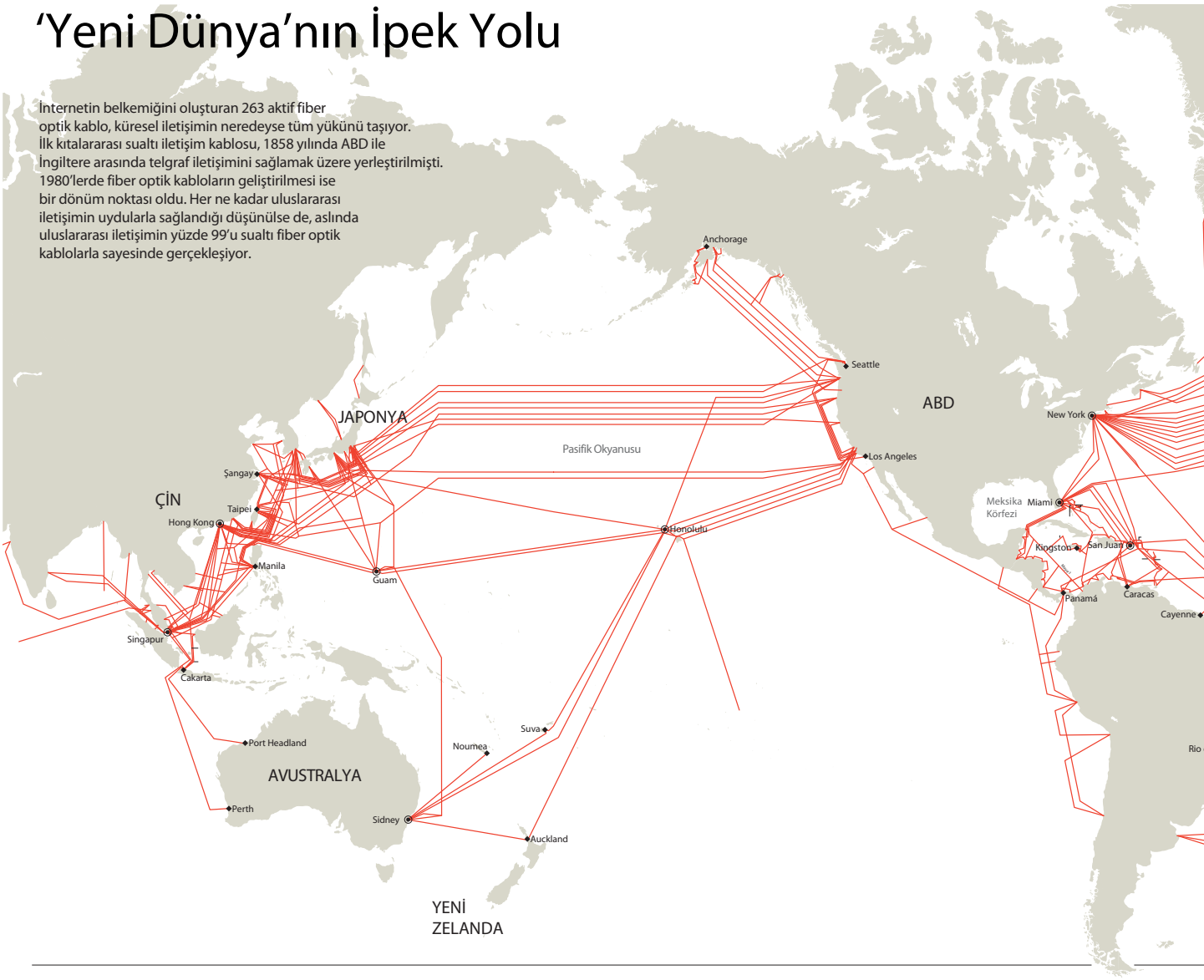
Fırsatlar ve yenilikler

7 milyar nüfuslu dünyamızda 2,5 milyar internet, 6,5 milyar ise cep telefonu kullanıcısı mevcut. Veri depolama maliyetlerinin teknolojik gelişmelerle neredeyse sıfıra yaklaşması ve iletişim araçlarının inanılmaz bir hızla yaygınlaşması, pek çok olumlu gelişmeyi beraberinde getirdi.

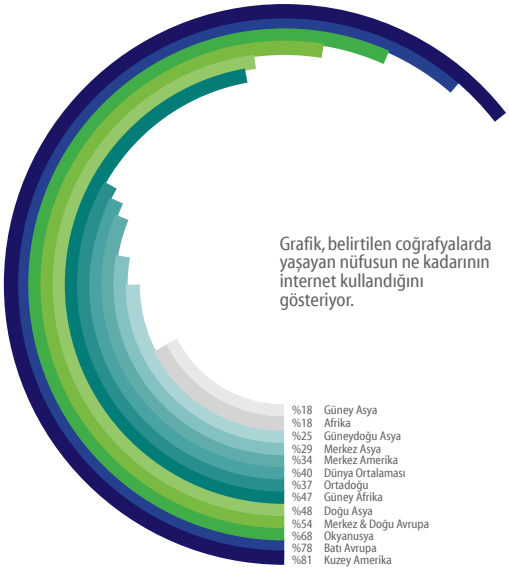
Öncelikle uluslararası iletişim maliyeti ciddi oranda azaldı. 1927 yılında New York-Londra arası 3 dakikalık bir görüşme 72 dolar iken, 1999 yılında bu rakam 0,3 dolara kadar düştü. Bunun yanı sıra, iletişimin kurulması için harcanan zaman da önemli ölçüde azaldı. İletişimin maliyeti, basitlik ve kullanışlılık bağlamında da kayda değer biçimde düşmüş oldu. Veri depolama ve iletişim kurma maliyetlerinde yaşanan bu değişim, oluşturduğu domino etkisiyle sosyal, politik ve ekonomik anlamda pek çok alana sirayet etti.

‘Yeni Dünya’nın İpek Yolu

İnternetin belkemiğini oluşturan 263 aktif fiber optik kablo, küresel iletişimin neredeyse tüm yükünü taşıyor. İlk kıtalararası sualtı iletişim kablosu, 1858 yılında ABD ile İngiltere arasında telgraf iletişimini sağlamak üzere yerleştirilmişti. 1980’lerde fiber optik kabloların geliştirilmesi ise bir dönüm noktası oldu. Her ne kadar uluslararası iletişimin uydularla sağlandığı düşünülse de, aslında uluslararası iletişimin yüzde 99’u sualtı fiber optik kablolarla sayesinde gerçekleşiyor.



İnternet Kullanım Oranı (Nüfus, %)



Kaynak: wearesocial.net

Dünya

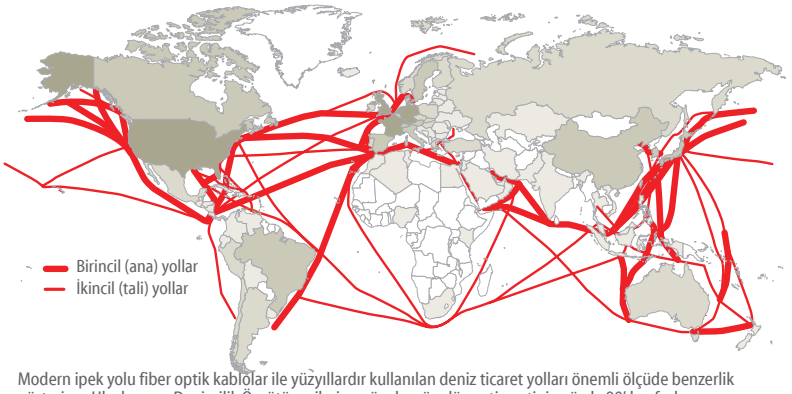
7.168.760.000 NÜFUS	%52 ŞEHİR	%48 KIRSAL	
2.905.000.000 İNTERNET KULLANICISI	%40 İNTERNET BAĞLANTI ORANI		
1.856.680.860 AKTİF SOSYAL MEDYA KULLANICISI	%25 SOSYAL MEDYA ARAÇLARINA BAĞLANMA ORANI		
7.000.000.000 AKTİF TELEFON KULLANICISI	%97 TELEFON ERİŞİM ORANI		

Türkiye

76.667.864 NÜFUS	%91,3 ŞEHİR	%8,7 KIRSAL	
35.990.932 İNTERNET KULLANICISI	%47 İNTERNET BAĞLANTI ORANI		
34.000.000 AKTİF SOSYAL MEDYA KULLANICISI	%44 SOSYAL MEDYA ARAÇLARINA BAĞLANMA ORANI		
69,600,000 AKTİF TELEFON KULLANICISI	%90 TELEFON ERİŞİM ORANI		

Kaynak: census.gov, TÜİK, Dünya Bankası, internetlivestats

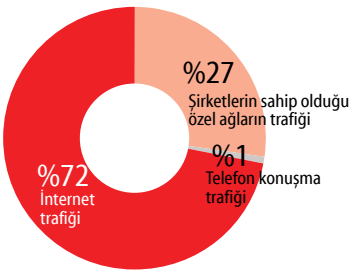
Küresel Deniz Ticaret Yolları



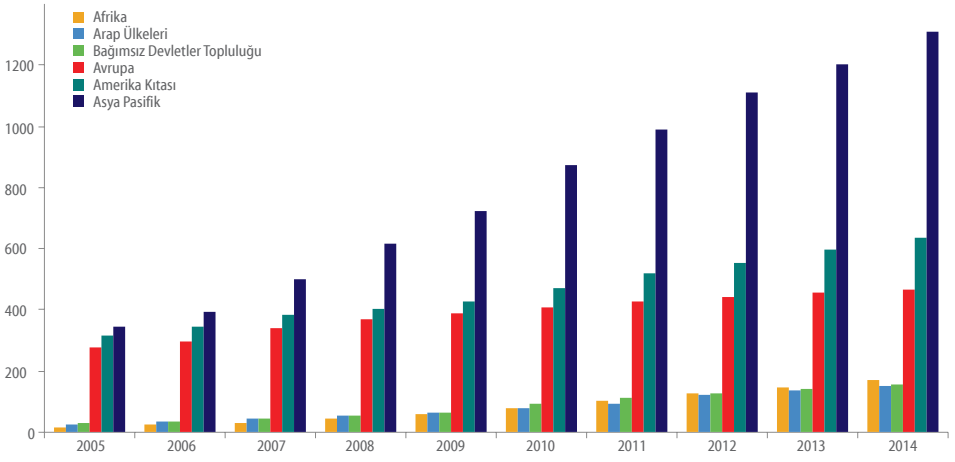
Modern ipek yolu fiber optik kablolar ile yüzyıllardır kullanılan deniz ticaret yolları önemli ölçüde benzerlik gösteriyor. Uluslararası Denizcilik Örgütü verilerine göre bugün dünya ticaretinin yüzde 90'dan fazlası, en uygun maliyetli taşımacılık yolu olan denizler üzerinden gerçekleşiyor.

Kablolardan Ne Geçiyor?

19. yüzyılda sualtı fiber optik kablolar sadece telgraf trafiği için kullanılıyordu. Sonraları ise telefon iletişimini sağlamak üzere farklı kablolar kullanıldı. Günümüzde ise fiber optik kabloların geliştirilmesiyle telefon, internet, özel verilerden oluşan dijital bilgilerin aynı anda, aynı hat üzerinden aktarılması mümkün oldu.

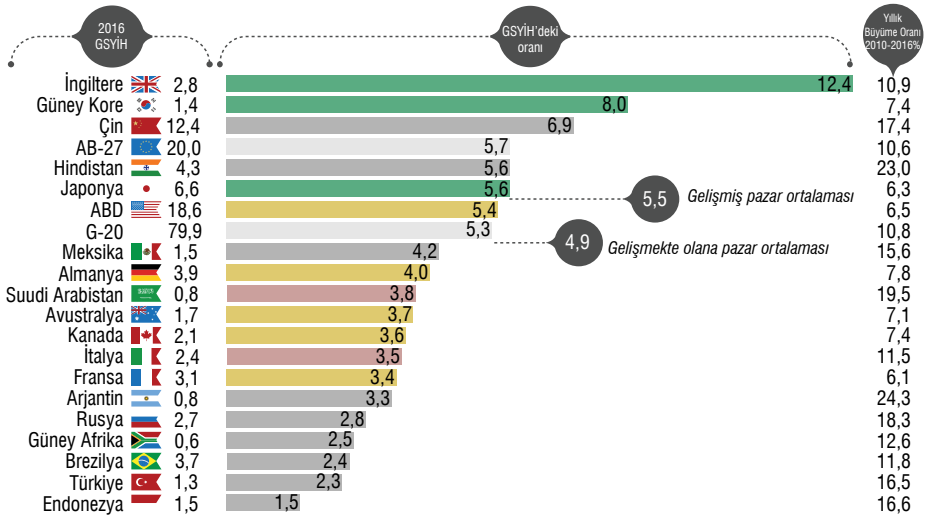


Yıllara Göre İnternet Kullanıcılarının Artışı



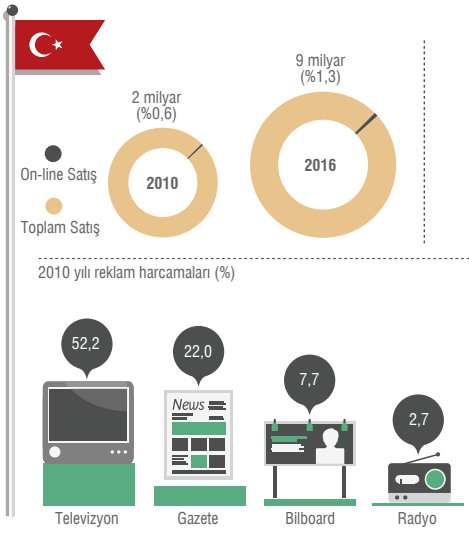
Kaynak: Uluslararası Telekomünikasyon Birliği

2016'da İnternet Ekonomisi G-20 Ülkelerin GSYİH Toplamında Yüzde 5,3'e Denk Gelecek



Kaynak: EIU, OECD, Ülke İstatistik Kurumları, BCG analysis.

İnternetin Ticarete Etkisi



Kaynak: EIU; Ovum, Gartner, Euromonitor International, OECD, Magnaglobal,

Öyle ki sadece iletişim alanında değil; diğer pek çok alanda da bilgisayar teknolojilerinin kullanılmaya başlamasıyla düşük maliyetli, kullanışlı ve basit sistemler ortaya çıkmaya başladı. Tek bir kimlik numarasıyla bireylerin neredeyse tüm verilerine erişilir oldu; su, enerji, finans, sağlık gibi kritik altyapıların idare ve organizasyonu kolaylaştı.

Öte yandan en genel ismiyle Siber-Fiziksel Sistemler (*Cyber-Physical Systems)* olarak bilinen yapılar ortaya çıkmaya başladı. Bu yapılara örnek olarak sağlık alanında kalp ritmi, vücut ısısı gibi verileri anlık olarak takip eden yardımcı sistemler; savunma alanında akıllı savunma sistemleri, insansız araçlar, uydu sistemleri, akıllı üniformalar ve araçlar; ulaşım alanında kendi kendine seyahat edebilen araçlar, interaktif trafik kontrol sistemleri, taşıtlar arası iletişim sistemleri gösterilebilir.

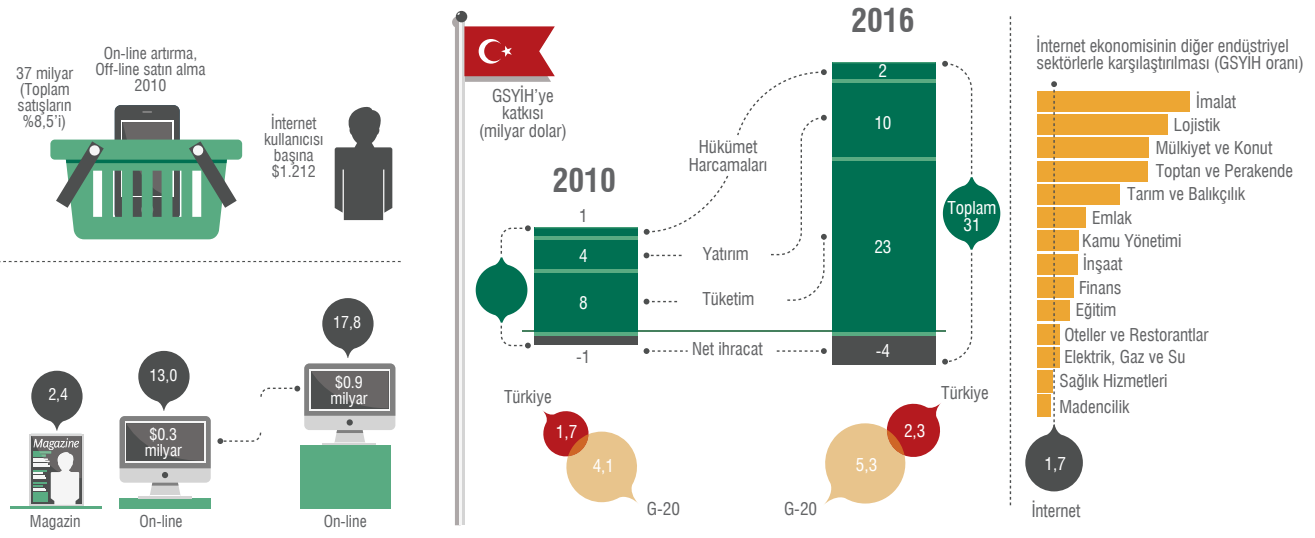
İnternet ekonomisi ya da dijital pazar

Bir iletişim aracı olarak ortaya çıkan ve buna uygun olarak tasarlanan internet, bireyler ile bilgi arasında önemli bir bağ kuran yapısıyla toplumları, kültürleri ve ekonomileri de etkilemeye başladı. OECD ülkeleri arasında artık su, elektrik, ulaşım ağlarıyla eşdeğer tutulan internet, dünya ekonomisi ve ülke ekonomileri açısından yeni bir fırsat penceresi açtı. 2008 yılında OECD tarafından yayınlanan *İnternet Ekonomisinin Geleceği* başlıklı bildiriye göre bu saha, "internet ve internetle bağlantılı bilgi ve iletişim teknolojileriyle gerçekleştirilen ekonomik, sosyal ve kültürel faaliyetler bütünü" olarak tanımlanıyor.

İnternet ekonomisinin büyüklüğü ve etkisi hesaplanırken internetle bağlantılı faaliyetlerin oluşturduğu katma değer (doğrudan etki), net GSYİH büyümesi (dinamik etki) ve tüketici fazlası ile refah kazanımları (dolaylı etki) gibi metrikler kullanılıyor. *The Boston Consulting Group* tarafından hazırlanan ve G-20 ülkelerini mercek altına alan çalışma, internet ekonomisi hakkında çarpıcı veriler sunuyor. 2010 yılı verilerine göre internet ekonomisinin büyüklüğü, G-20 ülkelerinin toplam GSYİH'sinin yüzde 4,1'ine (2,3 trilyon dolar) tekabül ediyor. Bu rakamın, 2016 yılında 4,2 trilyon dolara ulaşması öngörülüyor. Aynı araştırmaya göre, G-20 ülkelerinde internet ekonomisi her yıl yüzde 10'a yakın bir büyüme kaydediyor. Bu açıdan, eğer internet ekonomisi bir ülke ekonomisinin tamamını oluşturuyordu ülke ekonomileri sıralamasında ilk 5 içinde yer alacaktı. Dolayısıyla, gelişmiş ve gelişmekte olan ülkeler bu büyük pastadan pay almak için ikili, çok taraflı ve uluslararası anlaşmalar yapma yoluna gidiyor. Türkiye'de özellikle *e-ticaret* konusunda farkındalığın erken dönemde oluştuğunuz görüyoruz. 1998 Bilim ve Teknoloji Yüksek Kurulu elektronik ticaretin geliştirilmesi amacıyla dört temel hedef gerçekleştirdi. Bu hedefler, gerekli teknik ve idari altyapının kurulmasını sağlamak, hukuki yapıyı oluşturmak, elektronik ticareti özendirecek önlemleri almak ve ulusal politika ve uygulamaların uluslararası politikalar ve uygulamalarla uyumunu sağlamak olarak belirlendi. Bu hedeflerin her biri açısından değerlendirme yapmak mümkün. Ancak hukuki altyapının geliştirilmesi daha öncelikli Bu açıdan 2011 yılından bu yana Meclis'te bekleyen *Elektronik Ticaretin Düzenlenmesi Hakkında Kanun*'un bir an evvel çıkarılması gerekli.

Öte yandan, kuruluşu daha çok ekonomik amaçlara dayanan Avrupa Birliği'nin, üye ülkelerde yeknesak

Türkiye'nin İnternet Ekonomisi



CCB, TÜİK, World Economic Forum, BCG analysis.

Kaynak: EIU; Ovum, Gartner, Euromonitor International, OECD, Magnaglobal, CCB, TÜİK, World Economic Forum, BCG analysis.

uygulamaların yaygınlaşması ve böylece "dijital tek pazar" kurulması için uygulamaya koyduğu pek çok çalışma mevcut. Bu yıl "Dünyayı Yeniden Şekillendirme" teması ile toplanan *Dünya Ekonomik Forumu* tarafından çıkarılan "Dijital Altyapının Sunumu, Gelişen İnternet Ekonomisi" (*Delivering Digital Infrastructure, Advancing the Internet Economy*) raporunda ise dijital alanda ortaya çıkan hizmetlerin sosyal, politik ve ekonomik gelişmelerde itici bir güç oluşturduğu, yeni iş alanları açtığı, hatta yeni ve küresel bir "ipek yolu" oluşturduğu vurgulanıyor. Ayrıca raporda devletlerin kısıtlayıcı değil, özgürleştirici düzenlemeler yapmaları tavsiye ediliyor. Bu dijital ekosistem içerisinde servis sağlayıcılar, içerik sağlayıcılar (medya, IT şirketleri), donanım ve yazılım şirketleri, e-ticaret şirketleri (*Amazon, eBay* vb.) yer alıyor ki bu trilyonlarca dolarlık yatırım demek.

On-line haklar ve sosyal forumlar

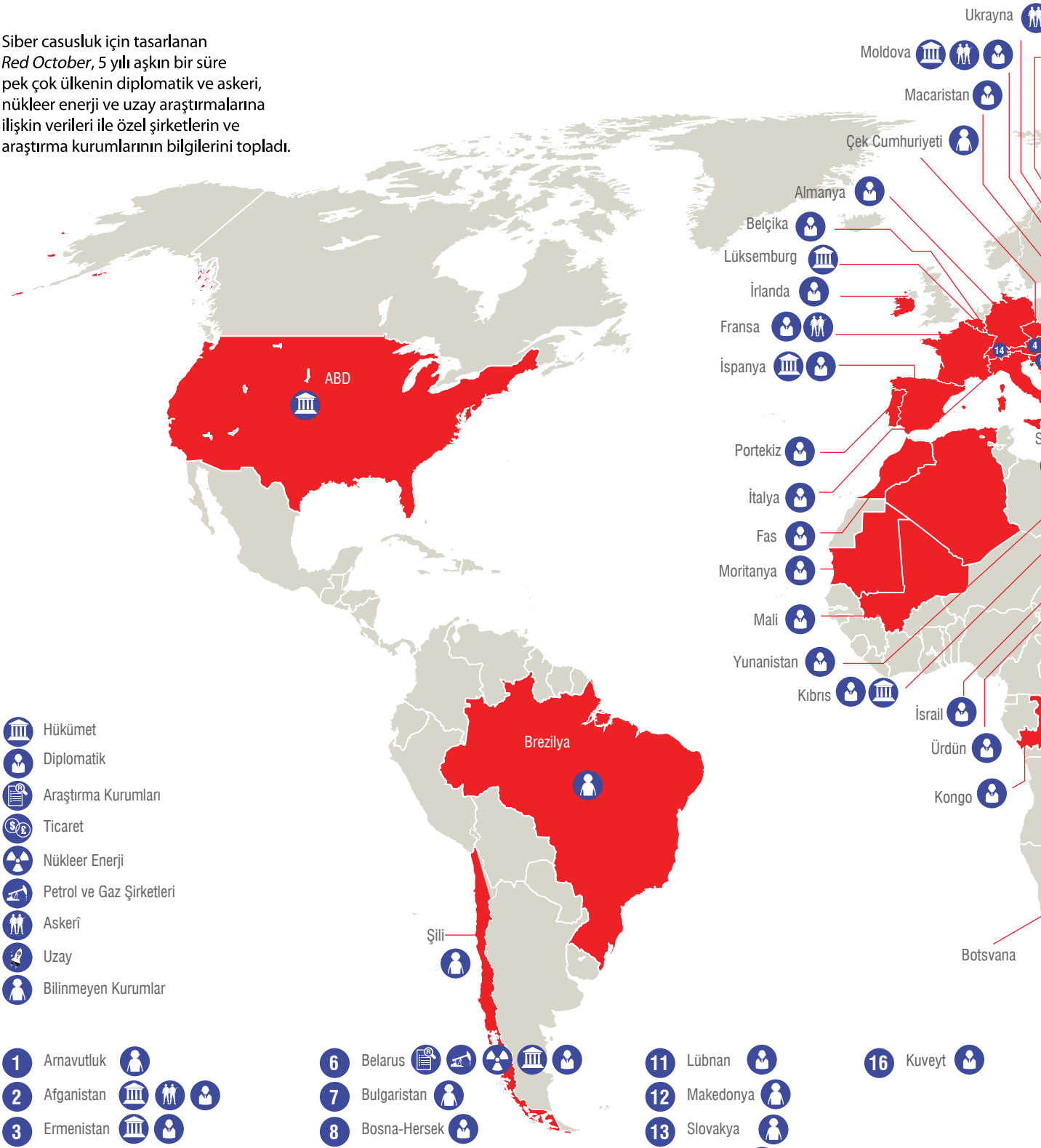
Teknolojik olarak bugün gelinen aşama, aslında belli bazı dönüm noktalarını tecrübe etmekle erişilmiş bir seviye. İlk dönüm noktasında, bilişim konusunda uzman olmayan kişilerin rahatlıkla yayın yapabileceği basit ve kullanışlı internet siteleri ve *blog* sayfaları bulunuyordu. İkinci olarak, bu siteler arasında bizlere optimum sonuçları sunan *arama motorları* teknolojisi gelişti. Üçüncü dönüm noktası, dijital ortama yüklenen içeriklerin entegrasyonuyla gerçekleşti. Şöyle ki yazıların paylaşıldığı internet sitelerinin yanı sıra müzik, video ve fotoğraf paylaşımı da inanılmaz bir hızla yaygınlaştı. Son dönüm noktası ise masaüstü bir bilgisayara bağlı kalmadan mobil olarak internete erişim araçlarının ortaya çıkışıyla yaşandı. Bu noktada, bireyler sosyal medya araçları üzerinden mobil olarak her an paylaşımda bulunabiliyor, genişletilmiş bir ifade özgürlüğü alanına sahip olarak kamuoyu oluşturabiliyor. Bu noktada *blog* sitelerinin (*Wordpress, Blogspot, Tumblr)*, sosyal medya araçlarının (*Facebook, LinkedIn*), mikroblog sitelerinin (*Twitter, Weibo*), on-line ansiklopedi sitelerinin (*Wiki)* ve son olarak içerik paylaşım sitelerinin (*YouTube, Flickr, Instagram*) politik ve sosyal tartışmaları etkileme ve şekillendirme gücü tartışmaya açıldı.

Blog sitelerinde yapılan paylaşımların nasıl bir etki uyandırdığını ilk olarak Afganistan ve Irak'ın işgali örneklerinde gördük. Koalisyon askerlerinin çektikleri fotoğrafları ve tecrübelerini günü gününe *blog* sitelerinde paylaşmaları, özellikle Amerikan toplumunda ciddi bir infiale neden olmuş ve ana akım medyanın güvenilirliğini ve politik kararların meşruiyetini sorgulamaya açmıştı.

Son olarak sosyal medya araçlarının etkin bir şekilde kullanılmasıyla oluşan etkiyi *Occupy Wall Street* hareketi, "Arap Baharı" süreci ve İspanya'daki *15-M* hareketi çerçevesinde gözlemleme fırsatı yakaladık. Sosyal medya ve sosyal hareketler üzerine yaptığı çalışmalarla tanınan Manuel Castells, bu olayların internet üzerinden yapılan paylaşımlarla mobilize olduğunu, internette doğduğunu, yaygınlaştığını, varlığını internet üzerinden devam ettirdiğini ancak "kamusal alanların işgali" olarak somutlaştığını belirtiyor. Dolayısıyla, sosyal medya araçları bir uyarıcı; eleştiri veya siyasal eylem ise bu uyarana bir cevap olarak ortaya çıkıyor. Öte yandan Malcolm Gladwell, sosyal medya araçlarının statükonun doğal bir düşmanı olmadığını, aksine mevcut sosyal ve siyasal yapıyı daha etkili bir forma dönüştüren araçlar olduğunu vurguluyor. Bu açıdan sosyal medya araçları, her-

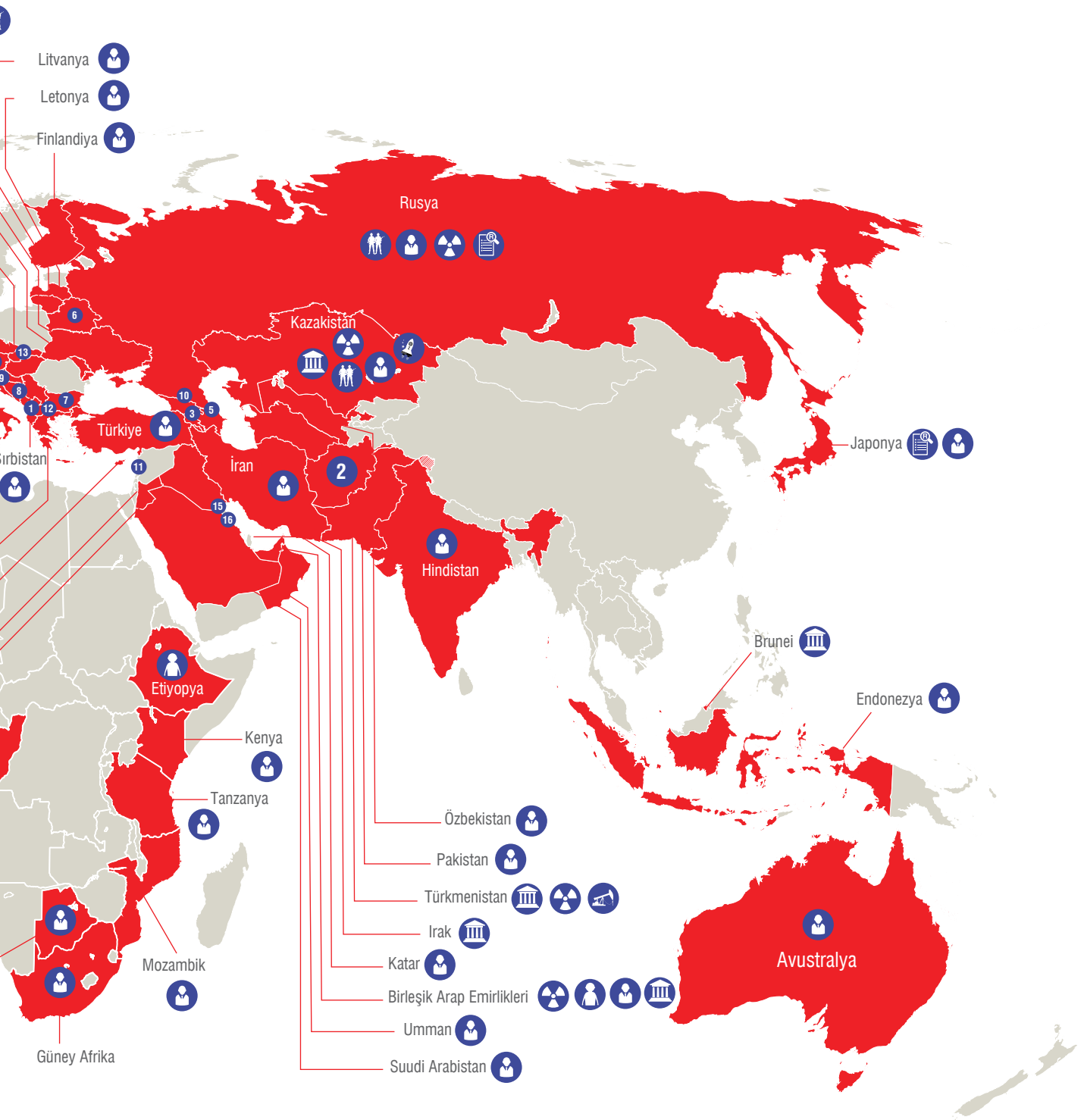
Siber Casusluk: *Red October*

Siber casusluk için tasarlanan *Red October*, 5 yılı aşkın bir süre pek çok ülkenin diplomatik ve askeri, nükleer enerji ve uzay araştırmalarına ilişkin verileri ile özel şirketlerin ve araştırma kurumlarının bilgilerini topladı.



1. Arnavutluk
2. Afganistan
3. Ermenistan
4. Avusturya
5. Azerbaycan
6. Belarus
7. Bulgaristan
8. Bosna-Hersek
9. Hırvatistan
10. Gürcistan
11. Lübnan
12. Makedonya
13. Slovakya
14. İsviçre
15. Bahreyn
16. Kuveyt

Kaynak: Kaspersky Lab.



Son zamanların en büyük siber casusluk girişimi olarak bilinen *Red October*, en az 5 yıl boyunca dünyanın birçok ülkesinde faaliyet gösteren bir casus yazılım. Bu süre içerisinde Microsoft Word ve Microsoft Excel'deki açıklardan faydalanarak ülkelerin diplomatik ve askeri bilgilerinden uzay teknolojisi projelerine kadar pek çok alandan bilgi toplayan Red October, bilinen en karmaşık ve uzun soluklu siber casusluk olayı olarak kabul ediliyor.

hangi bir talepte bulunmadan "anlamlı ve değerli" bir tepki ortaya koymayı sağladığı için bir çeşit illüzyon oluşturuyor. Örneğin, siyasal aktivizm pek çok fiziki tehlikeyi göze alarak meydanlarda bulunmayı içeriyorken, sosyal medya araçlarıyla oluşturulan atmosfer, böylesi bir tehlike unsuru içermiyor ve ciddi bir fedakârlıkta bulunmayı gerektirmiyor.

Ancak, reel dünyadaki etki alanı her geçen gün genişleyen siber alan, sunduğu fırsatların yanı sıra, sahip olduğu etki alanının suistimallere ve suçlara açık olması nedeniyle birtakım tehditler de barındırıyor. Öyle ki hem siber dünyada yeni tehdit unsurları ortaya çıkıyor hem de reel dünyadaki tehditler siber dünyayla uyum sağlayarak daha etkili bir meydan okumaya dönüşüyor. Siber alandaki gelişmeleri tam anlamıyla fırsata dönüştürebilmekse siber tehditlerin analiz edilerek gerekli önlemlerin alınmasından geçiyor.

Saniyede 12 kişi *siber suç* kurbanı

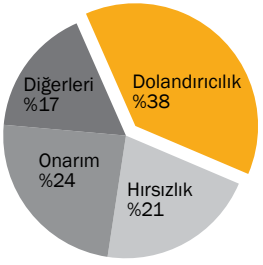
Özel ve genel internet ağları ya da kişisel bilgisayarlar vasıtasıyla işlenen "her türlü suç", *siber suç* kapsamında incelenebilir. Dolayısıyla kavram, yalnızca kişi ya da kurumların siber alanda uğratıldığı zararı değil, aynı zamanda internet ağları ve bilgisayarlar vasıtasıyla kişi ya da kurumların uğratıldığı reel zararları da kapsar. Örneğin, bir internet kullanıcısının bilgisayarındaki kişisel verilerin çalınması da internet bankacılığı yoluyla hesabında bulunan paranın çalınması da *siber suç* olarak kabul edilir.

Dünyanın en büyük yazılım şirketlerinden biri olan *Symantec*, yıllık siber güvenlik raporunda, siber alandaki son trendleri fırsatlar ve tehditler bağlamında detaylı bir biçimde ele alıyor. 2013 yılında yayınlanan son rapor, Türkiye de dâhil olmak üzere 24 farklı ülkeden 13 binin üzerinde internet kullanıcısı üzerinde yaptığı analizle, bu zamana kadar siber suçlar üzerine hazırlanan en detaylı rapor olma özelliğini taşıyor. Rapora göre, siber suçların yol açtığı zararın yıllık ortalaması 113 milyar dolar. Dünya genelinde siber suçlar nedeniyle mağdur olan kişilerin uğradığı ortalama maddi zarar ise 2012 yılından 2013'e kadar yüzde 50'lik bir artış göstererek 298 dolara ulaştı. Katılımcıların yüzde 38'i, son 1 yılda telefonları üzerinden siber suç kurbanı olmuş, son bir yılın toplam rakamı ise 378 milyon. Bu, saniyede 12 kişinin siber suç kurbanı olduğu anlamına geliyor.

Raporun ortaya koyduğu en çarpıcı sonuç ise şu: Akıllı telefon ve tablet kullananların yüzde 57'si, siber alandaki tehlikelere karşı tedbir alması gerektiğinin farkında bile değil.

Siber Suçlar
Yol Açtığı Yıllık Zarar

113 Milyar Dolar
2012 Londra Olimpiyatları bütçesinin **10 Katı**



%83
Kayıpların **%83**'ü **hırsızlık dolandırılıcılık** ve onarımdan kaynaklanıyor.

$298
Siber suçlardan mağdur olanların uğradığı **maddi zarar** (kişi başı)

%78
Son **4 yıl** içerisinde siber suçların **yüzde 78** oranında arttı.

$11,6
ABD'deki bir şirket yılda ortalama **100** başarılı siber saldırı yüzünden **11,6 milyon dolar** zarara uğradı.

%26
Geçtiğimiz yıldan bu yana, siber saldırıların yol açtığı zarar **yüzde 26'lık artış** gösterdi.

İnfografik: USAK

Siber saldırılarda yüzde 78 artış

Bilgisayar sistemlerini ve ağlarını hedef alan, kimi zaman yalnızca "zarar verme" kimi zaman ise hedef aldığı sistem ve ağı "yok etme" amacı güden saldırılar, siber saldırı olarak kabul ediliyor. Zararlı kodlar vasıtasıyla, hedef alınan bilgisayarların kodları, mantığı *(logic)* ve içinde yer alan verilerin değiştirildiği siber saldırılarla kimlik ve bilgi hırsızlığından bilgisayar sistemlerinin istismarına kadar pek çok suçun işlenmesi mümkün. Kötü amaçlı yazılım (*malware*), site trafiğinin yasal olmayan bir siteye yönlendirilmesi (*pharming*), kimlik hırsızlığı (*phishing*), istenmeyen e-posta (*spamming*), yanıltıcı e-posta (*spoofing*), casus yazılım (*spyware*), Truva (*Trojans*) ve virüsler gibi birçok yöntemle gerçekleştirilen ve bu nedenle siber suçların temelini oluşturan siber saldırılar, her geçen gün çeşitlenerek baş edilmesi daha güç bir hâl alıyor.

2012 ve 2013 yılları, siber saldırıların çokça gündeme geldiği ve medya görünürlüğünün arttığı bir yıl oldu. Örneğin, 2012 yılında başlayarak ABD'nin en önemli finans kurumlarını hedef alan siber saldırılar dizisi, kendilerini "Kâsım'ın Siber Savaşçıları" (*Qassam Cyber Fighters*) olarak tanımlayan bir grup tarafından "Müslümanların Masumiyeti" (*Innocence of Muslims, 2012*) adlı filme tepki olarak gerçekleştirildi. Teknoloji tarihinin en uzun soluklu siber saldırısı olarak kabul edilen bu saldırılar, 2013 yılında "Ebabil Operasyonu" (*Operation Ababeell*) ile deşifre edildi. Saldırılarını 4 ayrı safhada DDoS ataklarıyla devam ettiren grup, Amerikan finans sektörüne ciddi zararlar verdi.

Ponemon Institute ve dünyanın önde gelen bilgi teknolojileri şirketlerinden *Hewlett-Packard (HP) işbirliğiyle hazırlanan 2013 Cost of Cyber Crime Study* adlı çalışma, son 4 yıl içerisinde siber suçların yüzde 78 oranında artış

gösterdiğine dikkat çekiyor. ABD'den Japonya'ya kadar pek çok ülkeden 230 büyük şirket üzerinde yapılan araştırmalar sonucu hazırlanan rapor, ABD'deki bir şirketin yılda ortalama 100 başarılı siber saldırı yüzünden 11,6 milyon dolar zarara uğradığını ortaya koyuyor. Bu rakam, geçtiğimiz yıldan bu yana, siber saldırıların yol açtığı zararın yüzde 26'lık artış gösterdiği anlamına geliyor. Dolayısıyla siber saldırılar, etkisi ve zararı her geçen gün artan bir tehlike olarak karşımıza çıkıyor.

Devlet destekli *siber casusluk*

Bilgisayar ve internet ağları üzerinden kişisel ya da özel bilgilere, özellikle de devlet kurumlarının ya da çeşitli kuruluşların gizli verilerine erişilmesi ise siber casusluk kapsamında değerlendiriliyor. Neredeyse ilk bilgisayar sistemlerinin kurulması kadar eski bir geçmişe sahip olan siber casusluk girişimleri, özellikle 2012 yılındaki *Red October* vakasından sonra, bir güvenlik tehdidi olarak ciddi anlamda tartışılmaya başlandı. *Red October*, Ekim 2012'de fark edilen ve Ocak 2013'te Rus *Kaspersky Lab* firması tarafından deşifre edilen bir siber casusluk yazılımı. 5 yılı aşkın süre diplomatik ve askerî sırlardan enerji şirketlerinin veri tabanlarına kadar dünyanın farklı yerlerinden bilgi toplayan bu casus yazılım, bilinen en karmaşık ve uzun soluklu siber casusluk olayı olarak kabul ediliyor. *Red October*'la Türkiye'den de pek çok diplomatik ve kurumsal bilginin ele geçirildiği ifade ediliyor.

ABD'nin önde gelen teknoloji firmalarından *Verizon* tarafından hazırlanan *2014 Data Breach Investigation Report* ise siber casuslukla ilgili daha çarpıcı veriler ortaya koyuyor. 511 ayrı siber casusluk vakasını analiz eden rapora göre, siber casusluk en çok devlet kurumları ya da devlet destekli gruplar tarafından yapılıyor. Yüzde 87'si devlet destekli olan siber casusluk vakaları, devletlerin hem ülke içindeki çeşitli kurum ve sektörlerden hem de başka ülkelerin gizli diplomatik bilgilerinden haberdar olma isteğinden ileri geliyor. Zira siber casusluk eylemleri yüzde 80 ile 85 oranında iç verilere, sistemlerin işleyişine ve bu sistemlerde yer alan gizli bilgilerin içeriğine vâkıf olmayı amaçlıyor. Bu durum, siber casusluğun yakın gelecekte uluslararası ilişkilerde birtakım krizlere sebep olabileceğinin işaretçisi.

Mobil Siber Suçlar
Yol Açtığı Yıllık Zarar



%38

Son **1** yılda, cep telefonu kullananların **%38**'i siber suç mağduru oldu.

%27

Cep telefonu kullanıcıların **%27**'si mobil aygıtlarını kaybetti ya da çaldırdı.

378 Milyon Kişi

Yılda **378 Milyon Kişi** Siber Suç Kurbanı



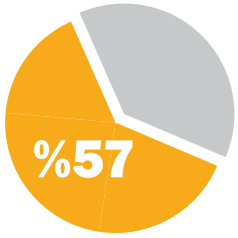
1 Milyon Kişi

Günde **1 Milyon Kişi** Mobil Siber Suç Kurbanı



12 Kişi

Saniyede **12 Kişi** Suç Kurbanı



Akıllı telefon ve tablet kullananların **yüzde 57**'si, siber alandaki tehlikelere karşı tedbir alması gerektiğinin farkında değil.

İnfografik: USAK

"Siber terörizm en büyük tehdit"

Pek çok farklı açıdan ele alınabilecek "siber terörizm", 1980 yılında Barry Collin tarafından kavramsallaştırıldı. Tıpkı reel dünyada olduğu gibi, siber dünyada da terörizmi tanımlamak oldukça güç. *Center for Strategic and International Studies*'in *(CSIS)* çalışmalarında siber terörizm "bilgisayar ağlarının kritik altyapılara (enerji, ulaşım vs.) zarar vermek ya da devre dışı bırakmak, devleti ya da halkı tedirgin etmek amacıyla kullanılması" şeklinde tanımlanıyor. Yani siber terörizm, siber alan vasıtasıyla gerçekleştirilen terör eylemlerini kapsıyor.

Reel dünyada aşina olduğumuz terör örgütlerinin siber dünyayı keşfetmesiyle beraber, siber terörizm de güvenlik gündeminde önemli bir yer teşkil etmeye başladı. Öyle ki 11 Eylül sonrasında Başkan Bush, Beyaz Saray bünyesinde *Siber Güvenlik Dairesi* kurup başına Terörle Mücadele Eski Koordinatörü Richard Clarke'ı atadı. Başkan Obama'nın da geçtiğimiz günlerde yaptığı bir açıklamada siber terörizmin ABD'nin karşılaştığı en büyük tehdit olduğunu ifade etmesi, ABD'nin siber terörizmden duyduğu endişeyi ispatlar nitelikte. Nitekim kritik altyapılarının yüzde 95'i elektrik altyapısına bağlı olarak çalışan ABD'nin elektrik altyapılarına yapılacak bir siber saldırı, ülke için bir kıyamet senaryosu anlamına geliyor.

Son tahlilde siber dünya, gözardı edilemeyecek büyüklükte bir zenginlik ve karmaşa oluşturdu. Bu zenginlik, geleneksel ekonomik, sosyal ve politik yapıları değişime zorluyor. Değişimin ve yeni fırsatların farkına vararak uygun strateji ve politikalarla bu zenginlikten pay almak ve fırsatları sürekli kılmak mümkün. Bahsi geçen tüm fırsatların yanı sıra; siber alan aynı zamanda siber suçlar, siber saldırılar, siber casusluk ve siber terör gibi birtakım tehditler için de zemin oluşturuyor. Siber alanın tam anlamıyla bir fırsata dönüştürülmesi ise siber tehditlerin farkında olunması ve bu tehditleri en aza indirecek tedbirlerin alınmasıyla mümkün olabilir. ■