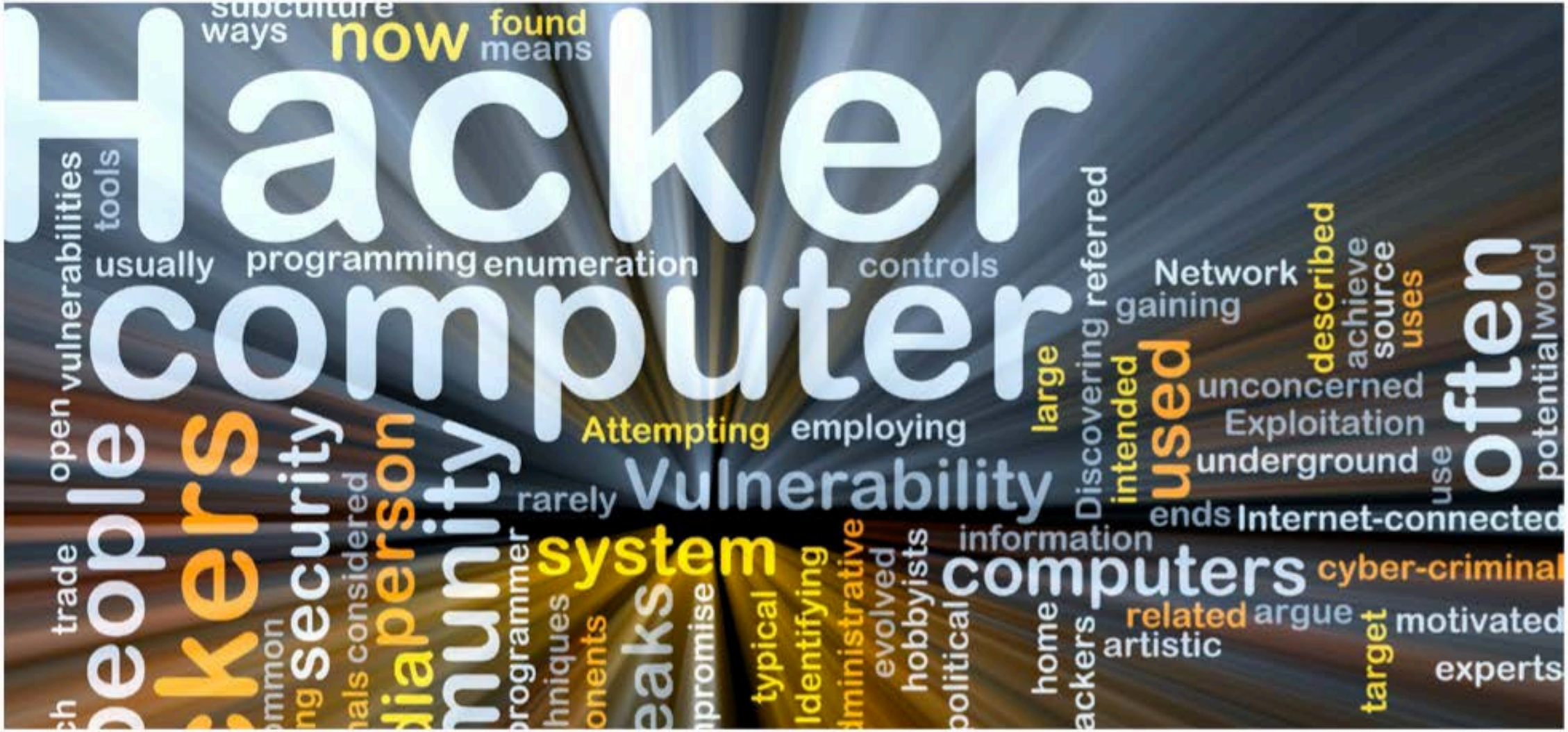
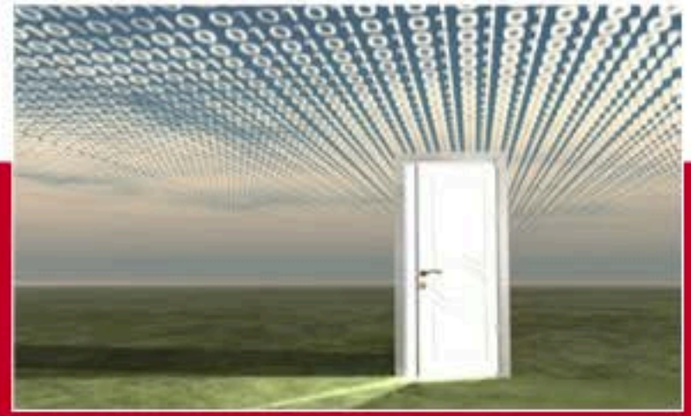
Bilgi Güvenliği



indeks:
indeks içerik-iletişim danışmanlık

Bilgisayar çağında bilgi toplumu

Her şeye sahip olabilirsiniz ama bilgisini elinde bulundurmadığınız hiçbir şeye hükmedemezsiniz. Bilgi toplumunda aktörler değişiyor, oyunun kuralları yeniden yazılıyor.



Tarihin akışını değiştiren 11 Eylül sonrasında küresel psikolojik savaşın ana hedefi bilgi ve istihbarat haline geldi. Bilginin en değerli silah olduğu yeni toplum modelinde, hayatımıza "bilgi güvenliği", "bilgi ekonomisi" ve "bilgi şebekeleri" gibi birçok yeni kavram dahil oldu. Dünya gündeminin stratejik bilgi üzerinde verilen mücadelelerce belirlendiği enformasyon çağında bilgi güvenliğini mercek altına alıyoruz.

İstihbarat tarihi birçok bilgi sızıntısı ve bunun sonucunda yaşanan krizlere tanıklık etti. Yaşanmış en büyük sızıntı skandallarından Watergate, bu konudaki en ünlü örneklerden biri. 1970'li yıllarda yaşanan ve ABD Başkanı Richard Nixon'ın istifasıyla sonuçlanan olayın üzerine gidilmesinde basının etkisi büyük oldu. Nixon'ın Demokrat Parti yetkililerini gizlice dinlettiğinin ortaya çıktığı bu olayın üzerine giden Washington Post muhabirleri

Yeni sorular, yeni tanımlar

İçerik devrimi yaşanıyor, internet teknolojisi bilginin kapsamını değiştiriyor. Stratejik sırlar, bilgi kaynakları ve başka pek çok şeye dair bildiklerimizi yeniden sorgulama zamanı!

Teknolojiyle entegrasyon süreci hayatımızda var olan birçok kavramı yeniden tanımlamamızı gerektirdi. Bir sürü soru yanıt bekliyor;

- **Bilgi nedir?**
- **Bilgi kime aittir?**
- **Bilgi güvenliği hangi noktada başlar ve biter?**
- **Stratejik sır olabilir mi?**

Bu soruların kökenini Antik Yunan'a kadar götürmek mümkün. Aristo'dan bu yana bilginin ne olduğunu tanımlamaya çalışıyoruz. Yeni olaylar ile bunlara karşı geliştirdiğimiz istihbarat önlemleri, bilgi güvenliği sistemleri... Yanıt vermekte ne kadar geç kaldığımızı gösteriyor.

İnternet teknolojisi, bilgiyi online hale getirdiği için, ona ulaşmak eskisine nazaran daha basit. 3G bağlantılı bir cep telefonuyla gelmiş geçmiş tüm istihbaratçılardan daha kolay bilgiye ulaşabiliyorsunuz. Kolay erişilebilmesine rağmen, sürekli değişen yapısıyla bilgiyi güncel olarak takip edebilmek zor! Mikro aktörlerin oluşturduğu ağ toplumuyla, kaynakların neredeyse sonsuza ulaşması, bilgiyi başıboş ve anonim kılıyor. Kimin çektiği belli olmayan bir fotoğraf çok önemli bir olayı belgelemeye yetebiliyor, kolektif üretilen içerik devrim yaratabiliyor.

"Gizlilik" etiketiyle sınıflandırılmış stratejik bilgilerin durumu da ayrı tartışma konusu. Özellikle istihbarat birimleri aracılığıyla topladığı bilgiyi saklamaya çalışan hükümetler, siber saldırılar karşısında sürekli tehdit altında. Son yıllarda yaşanan istihbarat sızıntıları büyük krizlere neden oldu. Krizlerin ardında bilgiye ulaşmak için birbiriyle mücadele halinde olan legal ve illegal örgütler bulunuyor. Mücadele özel hayatın sırlarını deşifre ederken, günbegün yayılan yeni izleme yöntemleri sayesinde sır, sır olmaktan çıkarak kamusallaşıyor.

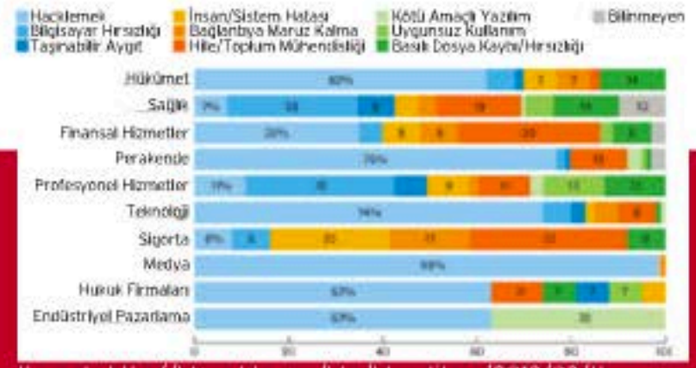
Bilgi güvenliği sözlüğü

Dünyadaki en zor şeylerden biri, herhangi bir bilgiyi saklı tutabilmek. Ulusal hükümetlerin istihbarat birimlerine milyarlarca dolarlık bütçeler ayırdığı ve siber örgütlerin en korunaklı verilere ulaşabilmenin yolunu bulduğu bir dönemde bilgiyi saklamak büyük başarı. İnternet teknolojisiyle, yeryüzünün herhangi bir santiminde iz bırakmadan bilgiyi tutabilmek mümkün değil.

Bilgiye ulaşmak için mücadele halindeki örgütlerin izlediği yöntemlerin başında internet casusluğu geliyor. Bilgi sızdırmaya yönelik faaliyetleri, yazılım ve donanım olarak iki ana başlık altında toplamak mümkün. Yazılım, işletim sistemi, programları; donanım ise yazılımın altyapısını oluşturan fiziksel cihazları kapsıyor. Verilerin bu unsurlardan sızdırılma biçimiyse

Sanal saldırılara karşı hazırlıklı ülkeler listesi

Kim verilerini kaybeder ve nasıl



Kaynak: http://blogs.hbr.org/hbr/hbreditors/2013/03/the_companies_and_countries_lo.html

Veri kaybı

Şirketlerin ve ülkelerin veri kayıpları kimi zaman sonuçları ekonomik olarak tahmin edilemeyecek zararlar yaratabiliyor. Rakiplerin eline geçtiğinde ciddi riskler doğurabilen veri kayıplarına dair kayıtları belirli başlıklar altında toplamak mümkün. "Deutche Welle Türkçe"de yayımlanan habere göre, internet kanalıyla yapılan sanayi casusluğu ve işlenen suçlar bütün dünyada her yıl 500 milyar dolarlık zarara yol açıyor.

- **Hack'leme,**
- **Bilgisayar hırsızlığı**
- **Toplum mühendisliği**

Araştırma şirketi KPMG'nin yaptığı bir çalışma bu konuda oldukça fikir verici. KMPG raporunun bir diğer bulgusu, veri hırsızlıklarının en fazla bürokrasiyi hedef aldığını gösteriyor.

Bir USB bellek neler yapabilir?

Kocaman kütüphanelere sığmayacak kadar geniş veriler, online ortamda rahatlıkla saklanabiliyor. Bir flash belleğe sığabilecek kadar sıkıştırılan dijital verilerin güvenle saklanması ise giderek zorlaşıyor.

Küresel internet kullanımının sonunda oluşan veri o kadar büyük ki Facebook'un 100 milyon kullanıcı barajını aştığı 2009 yılında küresel internet verisine dair ölçümler 14.414 PB'yi gösteriyordu. Bu ölçü, tüm verilerin kopyalanması için gereken standart DVD'lerin yan yana dizildiğinde Dünya'dan Ay'a kadar bir mesafeye uzanması anlamına geliyor. "Bu kadar geniş bir veritabanı içerisinde basit bir USB belleğe ne sığabilir?" diye düşünebilirsiniz. Ancak yaşanan deneyimler, bize bilgi sızdırma konusunda her detayı göz önünde bulundurmamız gerektiğini anımsatıyor.

ABD Savunma Bakanlığı Pentagon birkaç yıl önce bir düzenlemeyle bilgisayar kullanımında USB Bellek kullanımını yasakladığı ortaya çıktı. Sebebi merak edilen bu uygulamanın amacı daha sonra anlaşıldı. Pentagon 2008'de siber bir saldırıya uğramıştı ve bu saldırıda

Tarihsel bir dönüm noktası: Wikileaks

Stratejistlerin "ikinci 11 Eylül" vakası olarak tanımladığı Wikileaks yeni yüzyılın en büyük diplomasi krizlerinden birine neden oldu. Julian Assange ve arkadaşlarının kurduğu uluslararası organizasyon olan Wikileaks açık toplum düsturuyla, kamuoyuna birinci derecede önemli stratejik veriler sızdırdı. Ekim 2006'da Wikileaks adlı bir internet sitesinde yayına başlayan Assange'ın öyküsü Hollywood filmlerine ilham verdi. Enformasyon çağının ilk devrimi Wikileaks oldu.

Wikileaks'in dünya gündemini sarstığı ilk önemli vaka Nisan 2010 tarihinde yayınladığı bir video kaydı oldu. Bir Amerikan helikopterinden yapıldığı tahmin edilen kayıtta, Irak Savaşı esnasında Amerikalı askerlerin Reuters muhabirlerine ateş açtığı görüntüler yer alıyordu. Wikileaks temmuz ayında ABD Ordusuna ait 90 bin belgeyi sızdırmayı başardı.

Bir intikam operasyonu:

"Biz Anonymous'uz.
Orduyuz. Affetmeyiz. Unutmayız.
Bizi bekleyin."

Dünya genelinde tanınan ünlü hacker grubu Anonymous, 2008 yılından bu yana faaliyet yürütüyor. Kim oldukları konusunda bugüne kadar hiçbir bilgiye ulaşılamayan grup üyeleri düzenledikleri siber saldırılarla dünyanın önde gelen şirket ve ülke yönetimlerine zarar veriyorlar. Wikileaks'e hizmet vermekten vazgeçen şirketlerin peşine düşeceği yolunda tehditlerde bulunarak dikkatleri üzerine çeken Anonymous'un saldırılarından nasibini alan şirketlerden biri Mastercard oldu. Aynı dönemde, sosyal paylaşım sitesi Twitter'da "Operation Payback" (İntikam Operasyonu) adlı bir hesapta, Visa'nın sitesinin de çökertildiği mesajı yer aldı. Wikileaks'e yapılan bağışları engelleyen Paypal da saldırıya uğradı.

Japon elektronik devi Sony, 100 milyon kullanıcısının şahsi bilgilerinin çalınmasında dolaylı olarak Anonymous grubunun da payı olduğunu savundu. Sony, güvenlik ihlalinin ardından kimi kullanıcıların kredi kartı bilgilerinin de çalındığının anlaşılması üzerine sanal ortamda bilgisayar korsanlarını arayacak dedektifler kiraladı. Anonymous, şahsi bilgilerin çalınmasıyla ilgisi olmadığını açıkladı.

**Hatırla, 5 Kasım gecesini hatırla,
Barutu, ihaneti ve komployu...
Hiç bir neden bilmiyorum ki
gerektirsin,
Barut komplosunun
unutulmasını.
V**

Modern Robin Hood'lar

Anonymous, güvenlik konularına odaklı Amerikan düşünce kuruluşu Stratfor'a saldırı düzenledi. Austin merkezli kuruluş Stratfor, internet üzerindeki bütün faaliyetlerini durdurduğunu açıkladı. Anonymous, Stratfor'un müşterilerinin kredi kartı bilgilerini kullanarak farklı yardım kuruluşlarına bir milyon doların üzerinde bağış yaptığını açıkladı.

Anonymous Wikileaks'in yanı sıra Occupy Hareketi ve Arap Baharı'nın da destekçisi oldu. Kendilerini "özgürlük savaşçısı" ve "dijital Robin Hood" olarak tanımlayan hacker grubu güvenlik timlerince siber terörist olarak ilan edildi. Aralarında TC Başbakanlık sitesinin de bulunduğu birçok devlet kurumunun web sitesinin çökertilmesi eylemine adı karışan Anonymous zaman zaman, ulusal güvenlik sırlarının sızdırılmasına da hizmet etti. Örgütün Suriye Devlet Başkanı Beşer Esad'ın mail şifrelerini kırarak, iç yazışmalarını ifşa etmesi uzun süre konuşuldu.

Kızıl hackerlar Türkiye'de: Redhack

"Hak yiyen hack yer"

Bilgisayar korsanlığının en yaygın olduğu ülkelerden Türkiye, yakın zamanda, ünlü bir hacker grubuyla tanıştı. Kendilerine RedHack adını veren bir grup genç, devlet kurumlarına ait çeşitli sitelere saldırmaya başladı. Bu saldırılar kimi zaman erişimi kesmeye yönelik hack'leme olabildiği gibi, kimi zaman çeşitli gizli belgelerin sızdırılmasını da içerdi.

RedHack 1997 yılında kuruldu. O günden bu yana binlerce korsanlık eylemine katılan grup Şubat 2011'de Ankara Emniyet Müdürlüğü'nün gizli belgelerini ele geçirdi. Bu olay sonrasında Wikileaks tipinde bir sistem kurma kararı alan RedHack, popüler blog sitesi blogspot üzerinden bilgi dağıtımına geçeceklerini açıkladı.

Dijital iletişim döneminin yeni modellerinin Türkiye'ye yansıması ilk olarak Bilişim Suçları Soruşturma Bürosu'nu harekete geçirdi.

Vazgeçilmez maymuncuk:

1 2 3 4 5 6

Devletlerin siber sınavı

Dünya genelinde artan siber saldırılar gelişmiş ülkeleri çeşitli önlem arayışlarına itiyor. Bu konuda en ciddi kaygı duyanlardan biri de Avrupa Parlamentosu. Yakın bir zamanda siber suçlarla ilgili önemli bir direktifi oylayan AP, direktifi kabul etti. Direktifin ana amacı, AB üyesi ülkelerde bilgi sistemlerine yönelik yapılan saldırılar karşısında ortak bir tavır oluşturmak.

ABD yönetimi yakın zamanda ticari sırlarının çalınma vakalarında görülen artışla mücadele için geniş kapsamlı bir strateji açıkladı. Strateji; yurt dışında fikri mülkiyet hırsızlığını caydırabilmek için daha iyi bir koordinasyon tesis edilmesini içeriyor. Yakın zamanda ticari sır hırsızlığıyla ilgili olarak saldırıya uğrayan şirketlerin başında General Motors, Ford, DuPont, Dow Chemical ve Cargill geliyor.

İstihbaratta yeni dönem: PRISM

PRISM nedir?
ABD Ulusal Güvenlik Servisi'nin (NSA) kendi iç yazışmalarında kullandığı bir kod adı. Geçtiğimiz aylarda Guardian ve Washington Post gazeteleri tarafından ortaya çıkartılan bu program, NSA'ya Apple, Google, Microsoft ve Facebook gibi şirketlerin sunucularına doğrudan erişim imkanı tanıyor. NSA böylece milyonlarca kullanıcının kişisel bilgilerini, yazışmalarını ve görüntülerini arşivliyor.

Yeni "Soğuk Savaş"
ABD'nin başka ülke büyükelçiliklerini dinlediğinin ortaya çıkmasının ardından bilgi güvenliği tartışmaları alevlendi. Konuyla ilgili bir açıklama yapan Almanya Adalet Bakanı Sabine Leutheusser tepkisini "Kullanılan yöntem Soğuk Savaş sırasında düşmanlarımızın kullandığı yönteme benziyor" diyerek dile getirdi. Fransa Cumhurbaşkanı Hollande ise "casusluğun derhal sona ereceğine dair güvenceler olmadan müzakerelere başlanmayacak" dedi.

Henüz Wikileaks sızıntısının şokunun sürdüğü bir dönemde gündeme gelen PRISM iddiaları tüm dünyanın ilgisini üzerine çekti. Amerikan Ulusal Güvenlik Ajansı'nın (NSA, gizli bir istihbarat programı yürüttüğünü ortaya çıkaran ise eski bir CIA ajanı Edward Snowden oldu. Buna göre NSA, kendi başına bir bilgi merkezi olmuş ve neredeyse tüm dünyayı izleyen bir istihbarat ajansına dönüştü. Üstelik bu iddiaların vahameti başlangıçta düşünüldüğünden daha derin olduğu kısa bir süre sonra anlaşıldı.

Skandal Haziran 2013 tarihinde İngiliz Guardian Gazetesi'nin yayınladığı bir dizi haberle patlak verdi. Buna göre NSA başka ülke istihbarat servislerinin telefon kayıtlarını ve internet faaliyetlerini izliyordu. İlerleyen günlerde gazete, İngiliz hükümetinin fiber optik kablolar üzerinden yürütülen küresel iletişimi izleyerek çok büyük miktarda veriyi sakladığını açıkladı. Buna göre

Sızıntı örnekleri

Thomas Drake
Üst düzey bir NSA yöneticisi olan Thomas Drake, 2005 yılında Baltimore Sun gazetesine NSA'nın etkisiz, saldırgan ve aşırı maliyetli Trailblazer projesini geliştirdiğini açıkladı. Bu proje dinleme yoluyla elde edilen verilerin analiz programının geliştirilmesini kapsıyordu. Drake, söz konusu faaliyetlerinin yeni olmadığını ve kamuoyuna ulaşan kısmının ancak "buzdağının görünen yüzü" olduğunu söyledi. Drake, 10 ayrı suçtan 35 yıla kadar hapis istemiyle yargılandı. Drake'in bu süreçte aleyhindeki bütün davalar düştü. Yalnızca NSA'daki bilgisayarını yetkisini aşarak kullandığı suçlamasını kabul eden Drake'e, 1 yıl gözetimli serbestlik ve 240 saat toplum hizmeti cezaları verildi.

Shamai Leibowitz
Aslen İbranice alanında dil bilimci olan Shamai Leibowitz, FBI için çalışıyordu. Leibowitz, 2009 yılında bir blogger'a bilgi sızdırdığı için yargılandı. Sızdırdığı bilgiye göre, ABD uzun zamandan beri müttefiki olan İsrail'in Washington'da bulunan elçiliğini dinliyordu. Leibowitz görüşme kayıtlarını Amerika'da ünlü bir blogger olan Richard Silverstein'a sızdırdı.
Olayın ortaya çıkmasının ardından, yetkililer soruşturma başlatınca Silverstein, elinde bulundurduğu 200 sayfalık telefon kayıtlarını arka bahçesinde yakarak imha etti. "Çalışmam esnasında gücün istismar ve kanunların ihlal edildiği sonucunu bende uyandıran yanlışlıklarla

Jeffrey Sterling
Yakın zamandaki başka bir sızıntı örneği de eski CIA yetkilisi Jeffrey Sterling'in New York Times muhabiri James Risen'a Merlin Operasyonu ile ilgili bilgileri sızdırması oldu. Program Clinton hükümetinin İran'a nükleer silah programını sekteye uğratmak için hatalı silah tasarımlarını verme girişimini kapsıyordu. Olaydan sonra 43 yaşındaki Jeffrey A. Sterling'in aralarında adaleti engelleme ve ulusal savunma bilgilerini yetkisiz kişilere ifşanın da bulunduğu 6 suçtan yargılanacağı bildirildi. Olay ABD-İran ilişkilerini gererken, Sterling'in avukatı "Müvekkilimin herhangi birisiyle iş birliği yaptığı, bilgi aldığı veya hükümetten her hangi bir iş birliği yaptığı kanıtlanamaz" açıklamasını yaptı.