Defenderse del Espionaje Informático con Software Libre (1 año después de Snowden)"

Rafael Bonifaz – junio 2014

La Nube

¿Por donde viajan las comunicaciones?

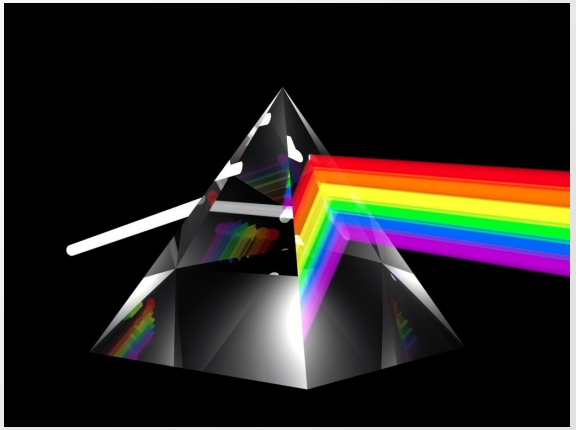
Imagen tomada de revista Wire online:
http://www.wired.com/politics/security/news/2007/10/domestic_taps

¿Cómo viaja la información?

- La información viaja por servidores y cables por el mundo
- La mayoría del tráfico de Internet es transparente y se puede espiar en cualquier punto
- Cuando se utiliza servicios pagados o gratuitos en la nube provistos por Google, Dropbox, etc... la información es compartida con estas empresas.
- Cuando se manda un correo a alguien con cuentas en Google, Hotmail, Yahoo, etc... la información queda disponible por estas empresas
- **“Si no pagas por el servicio, eres el producto”**

Revelaciones de Snowden

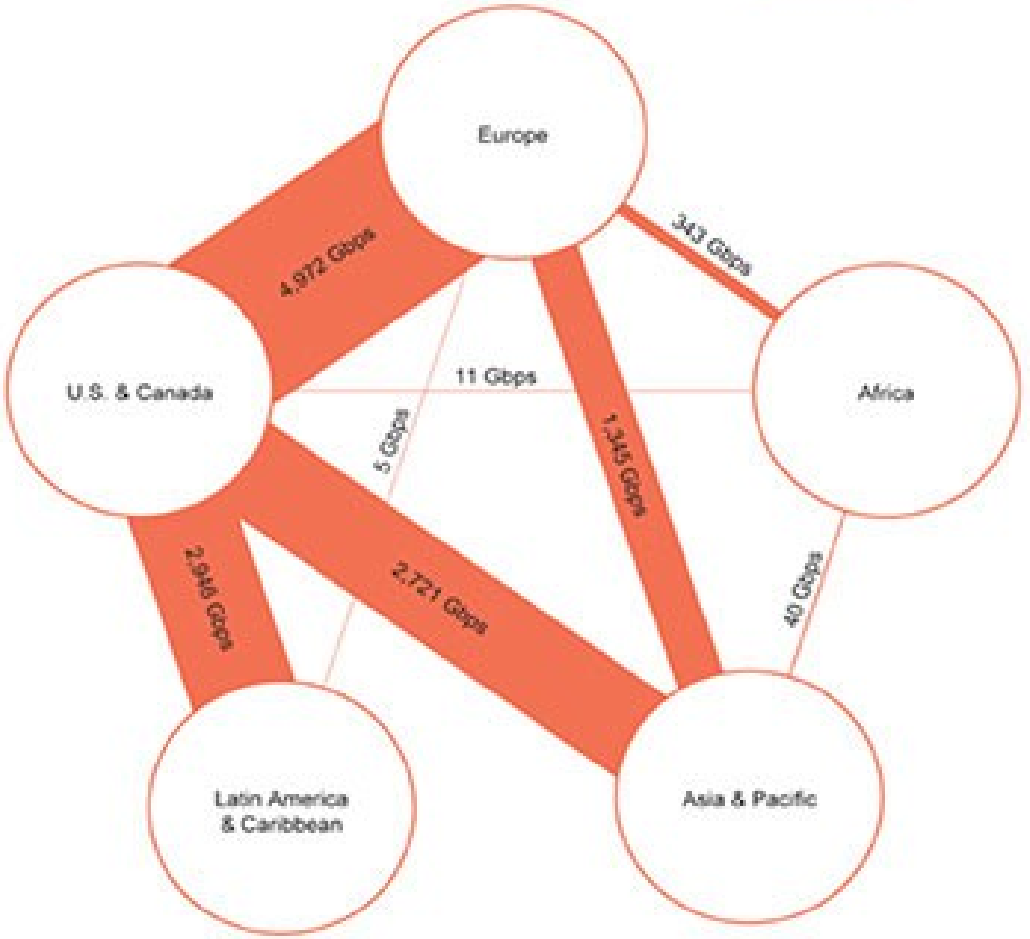
- NSA: Agencia de Seguridad Nacional (EEUU). Responsable de la inteligencia
- Programa PRISM muestra a empresas de Internet espiando a sus usuarios
- X-KEYSCORE buscador y recolector de datos del tráfico de Internet
- Todo lo que hacemos en Internet es constantemente vigilado y almacenado



(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

(TS//SI//NF) PRISM Collection Details

Current Providers

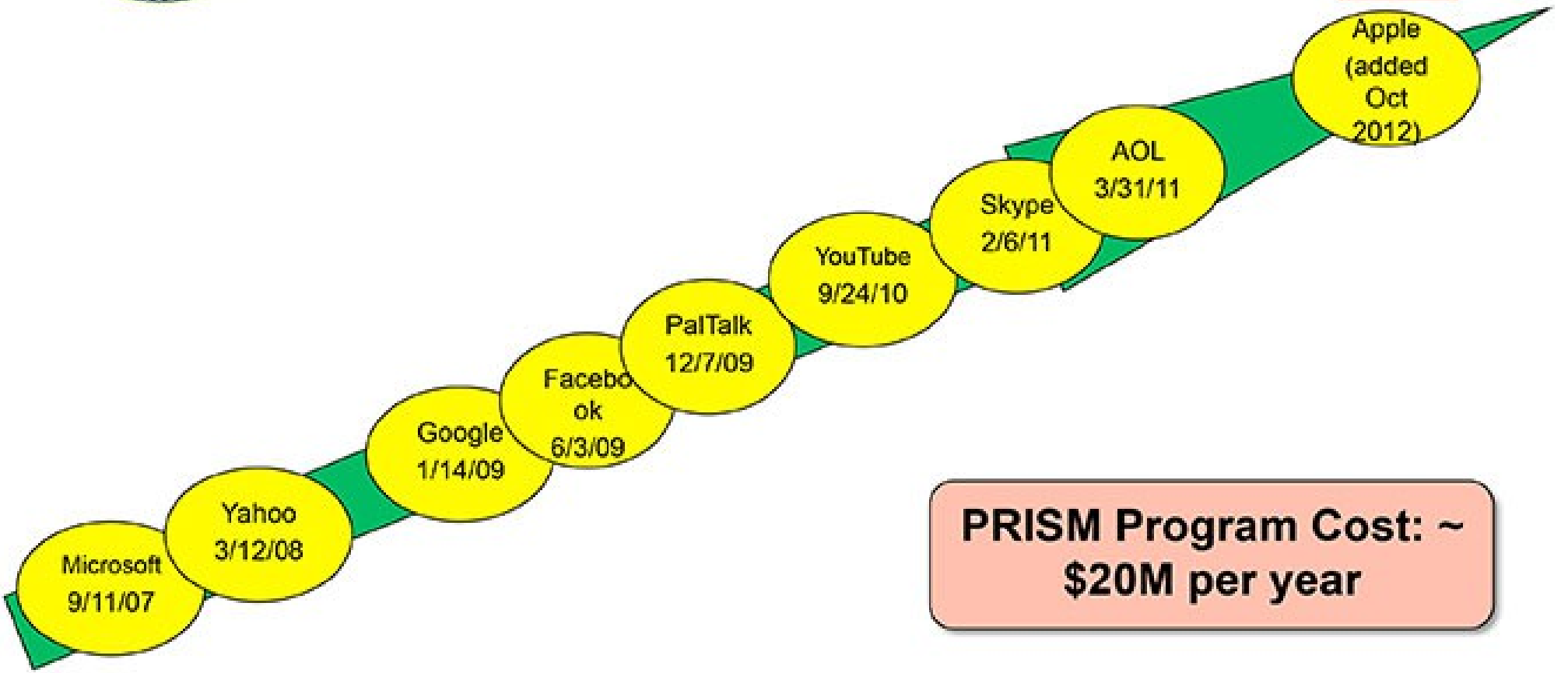
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ $20M per year

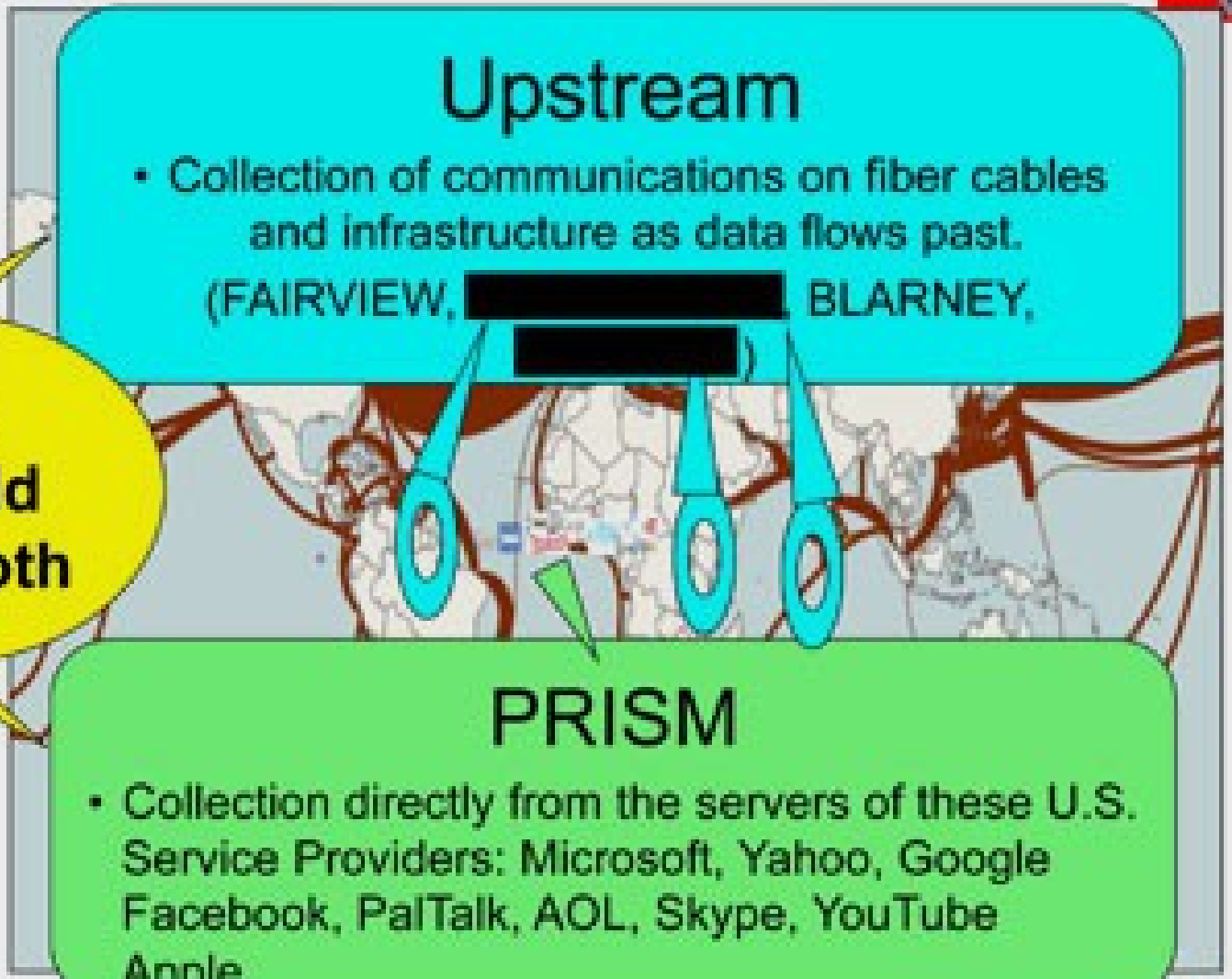
(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, [redacted], BLARNEY, [redacted])

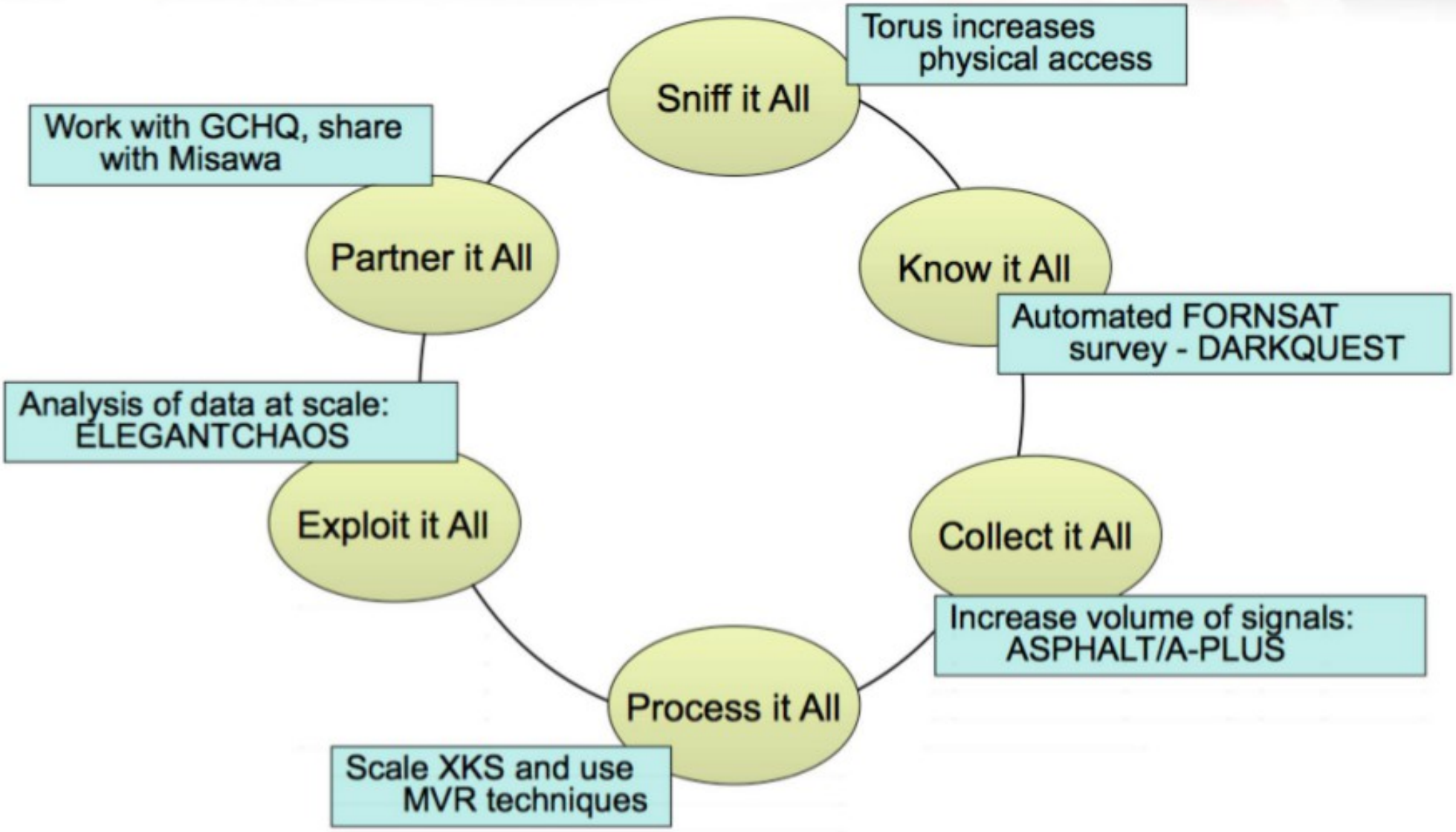


You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

New Collection Posture



NSA Strategic Partnerships

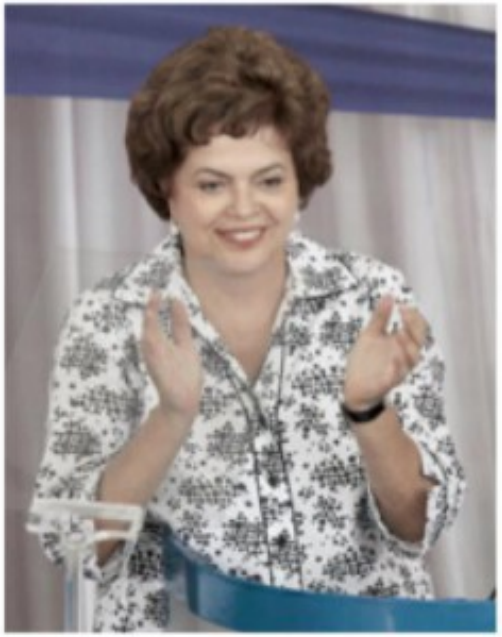
Alliances with over 80 Major Global Corporations Supporting both Missions

- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators

(U//FOUO) S2C42 surge effort

(U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.



Spyfiles de Wikileaks

- Publicadas en diciembre 2011
- Filtraciones hechas en países árabes
- Espionaje en Internet, celulares, computadoras
- Base del libro Cypherpunks
- http://wikileaks.org/spyfiles

FinSpy en PC

Tomado de http://wikileaks.org/spyfiles/list/document-type/video.html

FinSpy Celulares

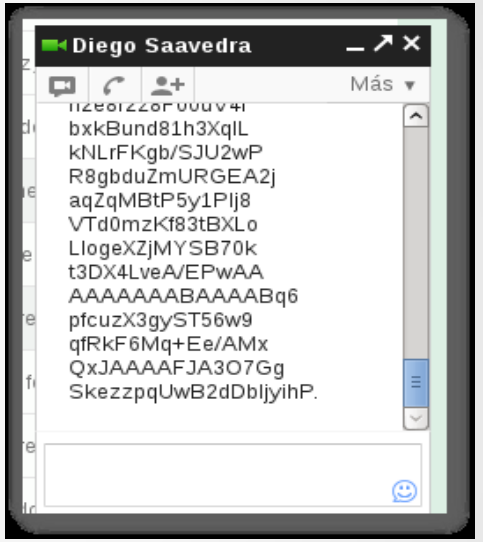
Tomado de http://wikileaks.org/spyfiles/list/document-type/video.html

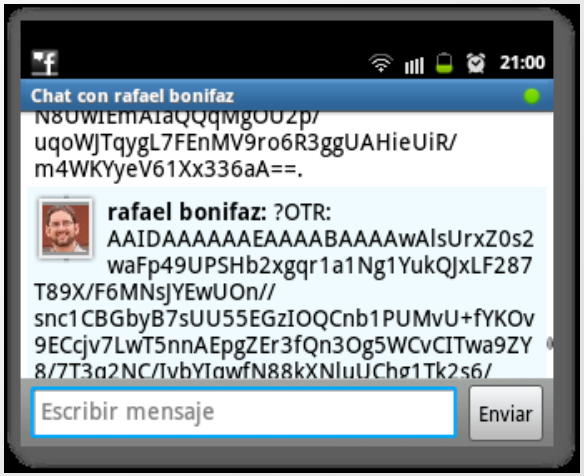
Infraestructura controlada y descentralizada

- Infraestructura controlada y descentralizada
- Hosting local accesible para todos
- Servidores propios de comunicaciones
- Correo postfix, exim, etc..
- Chat con XMPP, IRC
- VOZ/IP: Elastix, Asterisk, FreeSwitch
- Nube: Owncloud, Alfresco
- Celular: Firefox OS, Replicant OS, CyanogenMod
- Páginas web y servicios dentro del país
- Servicios ocultos con Tor

Criptografía

- Permite que la información sea accesible solo por los interesados.
- Los algoritmos más fuertes son los de llaves públicas y privadas
- Para encriptar correo se usa PGP: Soportado por cualquier cliente correo de software libre
- Para encriptar chat: OTR + Pidgin
- Para voz/ip: SRTP, IAX, VPNs
- Comunicación anónima y segura: TOR
- Transacciones monetarias: Bitcoin
- Pond alternativa al email





El Software Libre

- Se sabe como funciona
- Se necesita formar gente que entienda como funciona
- Se confía en una comunidad y no se lo hace de forma ciega
- La comunidad esta dispuesta a ayudar
- Para la comunidad el fin es tener el mejor software
- En criptografía significa ser lo más seguros
- Se puedo formar talento humano para apropiarse de la tecnología

Stinks (U)

[redacted]

CT SIGDEV

[redacted]

JUN 2012

Tor Stinks... (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

[redacted]

Software Libre, Criptografía y Privacidad

- Informarse:
  - Leer CypherPunks
    - http://assange.rt.com/es/episodio-8--assange-y-los-criptopunks/
    - http://assange.rt.com/es/episodio-9--assange-y-los-criptopunks/
  - Leer 1984 de George Orwell
  - Los Spyfiles
    - http://wikileaks.org/spyfiles
  - Confesiones de un Gangster Económico de John Perkins
  - Lean sobre PRISM y filtraciones de Snowden
  - No Place to Hide de Glen Greenwald

La situación actual

- La mayoría de la gente del mundo usa servicios Google, Yahoo, Microsoft, etc...
- Las redes sociales están fuera del país y pertenecen a empresas: Twitter, Facebook
- Las llamadas telefónicas son interceptarles
- El tráfico normalmente no esta encriptado
- El tráfico de Internet es guardado para cuando sea necesario
- No existe conciencia sobre estos peligros en la ciudadanía

A lo que se debe llegar

- Ciudadanos educados sobre los riesgos de las comunicaciones y la importancia de la privacidad
- Comunicaciones cifradas a nivel de clientes
- Uso de servicios descentralizados con software libre
- Terminales móviles y fijos con sistemas operativos libres
- Talento humano en capacidad de dominar tecnología
- Redes sociales libres y descentralizadas

¿Nuestra reacción?

- ¿Esta bien qué poca gente espíe a la población mundial?
- Debemos sensibilizar sobre el riesgo de perder la privacidad
- Debemos presionar y apoyar a nuestros gobiernos para tener independencia en nuestras comunicaciones
- ¿Qué opinan de la reacción de nuestros gobierno sobre PRISM? ¿UNASUR, CELAC?
- ¿Deben las universidades firmar convenios con las corporaciones de PRISM?

Constitución

- Art. 66.- Se reconoce y garantizará a las personas:
- 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

- 21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen.

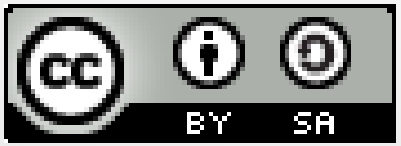
- *“Si quieres construir un barco, no empieces por buscar madera, cortar tablas o distribuir el trabajo, sino que primero has de evocar en los hombres el anhelo de mar libre y ancho.”*

Antoine de Saint-Exupéry

Gracias

- Rafael Bonifaz
- rafael@asle.ec
  - PGP ID: 5310523C
- @asle_ec @rbonifaz
- http://www.asle.ec http://rafael.bonifaz.ec

- ¡Copien y mejoren esta presentación!



El **Instituto Ecuatoriano de la Propiedad Intelectual - IEPI** con la intención de registrar y promocionar el desarrollo del Software Libre tiene el agrado de invitar a Usted al Lanzamiento de la Plataforma

www.minka.gob.ec

minka

Instituto Ecuatoriano de la **Propiedad Intelectual**

Día: miércoles 11 de junio de 2014.
Hora: 11h00 a 13h00
Lugar: Universidad Técnica Particular de Loja, Auditorio Oskar Jandl, San Cayetano Alto, Calle París. Loja

Confirmaciones: Geovanny Coloma (02)2903268 - 0987832403
Email: gjcoloma@iepi.gob.ec