Observaciones del espionaje en Internet de la NSA de EEUU

León Alberto Ramos Mendoza

Escuela Mexicana de Escritores

"...las tres consignas del Partido:
LA GUERRA ES LA PAZ
LA LIBERTAD ES LA ESCLAVITUD
LA IGNORANCIA ES LA FUERZA"
George Orwell

Diciembre 2016

Agradecimientos

Quiero dar especial agradecimiento a Lupita, mi esposa, por apoyarme en todo momento a revisar el presente ensayo. Creo que sus aportaciones para utilizar un lenguaje sencillo y digerible, potencian su alcance. Así mismo, quiero agradecer a Hiram Camarillo, consultor de seguridad y amigo, quien me ha apoyado realizando observaciones técnicas con un punto de vista fresco y acertado.

Índice

Introducción

El miércoles 5 de junio del 2013 aparece en *The Guardian*, un periódico británico, un artículo que expone la entrega de los registros de llamadas telefónicas, por parte de Verizon, a la Agencia de Seguridad Nacional de los Estados Unidos de América. Es la primera filtración de información clasificada que realiza Edward Snowden, un contratista externo de Booz Allen Hamilton, a los periodistas Glenn Greenwald, Ewen MacAskill y Laura Poitras.

No se conoce el número de archivos secretos, de la NSA y otras agencias, que Edward Snowden tiene en su poder, algunos estimados son de 1.7 millones de documentos. Edward, por su parte, tampoco supondría lo que su serie de filtraciones cambiarían en la percepción de la privacidad de la información electrónica; algunos afirman que ni el mismo George Orwell hubiera podido imaginar semejante invasión a la privacidad en su novela *1984*, en donde el gran hermano, ícono de los fundadores del partido autoritario en el poder, vigila a todos y cada uno de los clase medieros a través de telepantallas y micrófonos escondidos.

El presente ensayo tiene como objetivo dar un vistazo de acercamiento a algunos de los métodos de espionaje electrónicos utilizados por la NSA, tanto en redes de voz como de datos. Me es importante ofrecer una panorámica de dichos métodos porque, únicamente así, entenderemos el nivel de acceso a datos privados que EEUU tiene sobre todos los usuarios del mundo. Traté de concentrar el presente ensayo sólo en documentos generados por la Agencia de Seguridad Nacional de EEUU, sin embargo, complementé con otras fuentes algunos puntos importantes.

Los primeros apartados tratan de explicar el funcionamiento de los métodos, los subsecuentes esbozan el reto del almacenamiento y de la interpretación de la información. La parte final del ensayo presenta, lo que a mis ojos son, las posibles implicaciones, económicas, políticas y técnicas de dichas filtraciones.

1. Inteligencia de señales

Se le conoce a la inteligencia de señales, como la acción de obtener información de inteligencia, por medio de la intercepción de comunicaciones. Cuando se intervienen las señales de comunicación entre individuos, se le conoce como *Inteligencia de Comunicación* (COMINT) y, cuando se intervienen comunicaciones entre equipos, sin remitente y destinatario humano, se le conoce como *Inteligencia Electrónica* (ELINT).[1]

2. Métodos de espionaje utilizados

Describiré brevemente los métodos de espionaje utilizados por la NSA para obtener información de inteligencia. La información presentada fue recabada de artículos electrónicos de varios periódicos, medios que utilizó Edward Snowden para filtrar documentos secretos de varias organizaciones gubernamentales de EEUU.

Captura de metadatos

Los metadatos son los datos aparentemente impersonales sobre la actividad en Internet o en la red telefónica. Por ejemplo, si realizamos una llamada telefónica, los metadatos serían: El número remitente, número destino, fecha, hora, duración, tipo de dispositivo utilizado (vg: Samsung 5s).

En general existen metadatos en casi todos los medios electrónicos, la siguiente lista explica algunos metadatos que pueden obtenerse de varios servicios de Internet:

- **Telefonía**: El número remitente, número destino, fecha, hora, duración, tipo de dispositivo utilizado.
- **Páginas en Internet:** Dirección IP remitente, IP destino, fecha, hora, tipo de tráfico, tipo de navegador utilizado, tipo de equipo utilizado.
- **Fotografía**: Modelo de cámara, Apertura de diafragma, tiempo de exposición, profundidad de campo, flash.

1Department of the Army. (2004). Signals Intelligence. 2016, de Department of the Army Sitio web: http://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap8.htm

- **Correo electrónico**: Remitente, Destinatario, Servidor fuente, Servidor destino, encabezado y tipo de contenido.
- **Listas de contactos**: Nombre, teléfono y correo electrónico.

Aparentemente estos datos son inocuos y no revelan la identidad del remitente o el destinatario, tampoco se conoce el contenido de la información intercambiada, sin embargo, dichos datos pueden aportarnos pistas suficientes para descubrir los hábitos, y por ende, el perfil de la persona que lo usa.

Geolocalización de celulares y equipos

El esfuerzo de ubicación geográfica de equipos conectados a las redes GSM (redes de voz y datos móviles), se realiza en tres aristas principales: Ubicación de SIM por triangulación, Drones con antenas transmisoras, Filtración de IP del dispositivo.[2]

Ubicación de SIM por triangulación

La tecnología con la que funciona el celular, utiliza una o varias antenas celulares a la vez, así un teléfono puede mantener una llamada telefónica en movimiento enlazándose a la célula con mayor intensidad. La NSA y otras agencias, utilizan su acceso a los equipos instalados en las antenas para triangular la ubicación geográfica de los celulares.

Cabe mencionar que por el simple hecho de encender el dispositivo y contar con señal, el equipo puede ser susceptible a rastreo.

Drones con antenas transmisoras

Ya hemos hablado anteriormente sobre la triangulación de celulares por medio de las antenas, sin embargo, en algunos casos, es más sencillo tener acceso directo a la ubicación del equipo y a su información. Lo anterior es logrado mediante el montaje de una antena celular móvil sobre drones controlados. De ésta forma, si un equipo no cuenta con cobertura, o la triangulación es incierta, los drones pueden hacerle llegar una antena disponible.

2BRUCE SCHNEIER. (2014). Everything We Know About How the NSA Tracks People's Physical Location. 23/11/2016, de The Atlantic Sitio web: https://goo.gl/Jh82sy

Filtración de IP del dispositivo

Muchas aplicaciones para smartphones, envían la dirección IP del dispositivo en caso de estar conectado a Internet, así la NSA, utilizando una lista de relación entre IPs y ubicaciones, puede enriquecer la ubicación geográfica.

Cripto-análisis

El cripto-análisis es una serie de métodos que se utilizan para romper comunicaciones que están cifradas, es decir, que no son evidentes y son ilegibles de primera instancia. Actualmente, cuando un individuo, empresa u organización, necesita enviar información privada utiliza el cifrado. Dicho cifrado se soporta en un modelo matemático de una sola vía, se usan contraseñas, certificados y datos aleatorios, para, a través de cálculos matemáticos, generar un resultado que no puede ser decodificado en forma inversa.
Extracto de correo electrónico cifrado: *wcBMA/cvNCJcSBjSAQf9FTxyA06Gibk*

Ruptura de comunicaciones cifradas

Uno de los algoritmos matemáticos más populares utilizados para el cifrado de datos es el *intercambio de llaves criptográficas de Diffie-Hellman*. Como se mencionó anteriormente, la ruptura de los códigos generados por dicho algoritmo, en teoría, necesitaría varios años de procesamiento de datos en un equipo de alto desempeño, sin embargo, nuevos estudios revelan una falla en el algoritmo Diffie-Hellman que permite, romper las comunicaciones, al acotar el universo de números primos utilizados para el cifrado.

Según el estudio *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*[3], la NSA comprometió al 82% de los servidores web HTTPS al utilizar cadenas de cifrado de tan sólo 512bits. Esto es el 7% del millón de páginas más populares de Internet. En el caso de las cadenas de 1024bits, aprovechando el universo acotado de números primos, se puede romper el 18% de los sitios más populares en Internet.

3David Adrian, et al.. (2015). Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. 28/11/2016, de WeakDH.org Sitio web: https://goo.gl/gvKQ4J

Para el caso de las comunicaciones seguras entre particulares como: VPNs IPSEC y accesos SSH, la NSA puede tener comprometidos hasta el 66% y 26% respectivamente.

La ruptura de lo que anteriormente se consideraba como privado, provoca un cambio en el paradigma establecido, ya que gran parte de nuestras actividades en Internet se construyeron con la base en la privacidad de ciertas comunicaciones. Lo aterrador de esta confirmación, no es que la NSA tenga la capacidad de hacerlo a voluntad, lo aterrador es que cualquier otra organización pueda lograrlo si cuenta con la motivación suficiente.

Acuerdos con terceros

El uso de métodos propios para el espionaje, conlleva un gasto importante de recursos como: Poder de procesamiento, inversión en equipo, personal especializado, cobertura geográfica.

De acuerdo con los boletines revelados por Edward Snowden, la agencia NSA, implementó varias estrategias adicionales para incrementar su espectro de acción. Según el artículo Driver 1: Worldwide SIGINT/Defense Cryptologic Platform[4], observamos la distribución global de puntos geográficos en donde las comunicaciones son desencriptadas, gran cantidad de esos puntos se encuentra en zonas extraterritoriales para EEUU. El mismo artículo revela que existen alianzas con terceros, agencias regionales, y equipos implantados.

La ubicación de los puntos de extracción criptográfica se explica, por la gran dependencia que los servicios de Internet tienen de la infraestructura americana, la mayoría de los enlaces de fibra óptica intercontinentales y servidores se encuentran convenientemente en algún punto de Estados Unidos de América.

4National Security Agency. (2012). Driver 1: Worldwide SIGINT/Defense Cryptologic Platform. 23/11/2013, de NRC Sitio web: https://goo.gl/CQKQ18

El resto del país y zonas de importancia geopolítica, se cubre con acuerdos, ya sea con otras agencias de inteligencia, o bien, con proveedores de servicio y, en el peor de los casos, el acuerdo con fabricantes de equipo permite instalar productos con “puertas traseras”.

Acuerdos con otras agencias

En los artículos *US, German SIGINTers Increase Cooperation on African Targets*[5] y *NSA Intelligence Relationship with Israel*[6] se puede conocer el modo de operación para la generación de alianzas con otras agencias de inteligencia, específicamente, con la contraparte de Inteligencia de señales.

Es así, que ambas agencias pueden disfrutar de información compartida, claro, desde un punto de vista asimétrico, es decir, la NSA comparte menor información de la que recibe. Como podemos ver en el artículo *NSA Intelligence Relationship with Israel*, en donde, la ISNU (Israel SIGINT National Unit), se queja de no recibir suficiente información y cooperación por parte de la NSA, es de suponerse una relación similar con la ESOC (European Security Operations Center) y con el resto de agencias en el mundo.

Inclusive, la política de secrecía de la NSA queda al descubierto en el memo de cooperación entre Gran Bretaña y EEUU en el documento: *British - U.S. Communications Intelligence Agreement Memo*, en donde se genera el proyecto *UKUSA*, se puede observar el siguiente párrafo:

> b) (S//NF) Unilaterally by the Signals Intelligence Directorate: When sharing the planned targeting information with a Second Party would be contrary to U.S. interests, or when the Second Party declines a collaboration proposal, the proposed targeting must be presented to the Signals Intelligence Director for approval with

5National Security Agency. (2007). US, German SIGINTers Increase Cooperation on African Targets. 18/06/2014, de Der Spiegel Sitio web: https://goo.gl/IQf5u6
6National Security Agency. (2013). NSA Intelligence Relationship with Israel. 03/08/2014, de The Intercept Sitio web: https://goo.gl/tLp25t

> justification for the criticality of the proposed collection. If approved, any collection, processing and dissemination of the Second Party information must be maintained in NOFORN channels.

En donde los acuerdos de cooperación, aún rechazados por los gobiernos y agencias de terceros, se mantendrán clandestinamente en canales no formales, siempre y cuando la criticidad de los datos para EEUU lo justifique.

Acuerdos con proveedores de servicio

La mejor manera de espiar las comunicaciones extranjeras, es mantener pocos enlaces de datos submarinos de América continental al resto del mundo. Dichos enlaces son fundamentales, ya que la mayoría de los servicios en Internet, se encuentran hosteados en EEUU. Es así que casi cualquier actividad de navegación del mundo, es forzada a atravesar la infraestructura de espionaje de EEUU colocada en los enlaces submarinos. (*Driver 1: Worldwide SIGINT/Defense Cryptologic Platform*)

Son los acuerdos con los proveedores de servicio, los que logran, a través de la instalación de equipo propio en puntos geográficos extraterritoriales, o bien, mediante la adopción de políticas de compra de productos que incrustan dentro de los equipos los métodos de espionaje.

Por otro lado, uno de los mayores escándalos derivados de la liberación de Edward Snowden de los documentos de la NSA, es el proyecto PRISM[7]. Dicho proyecto se encarga de recopilar información, no desde los metadatos, desde la fuente misma de los servicios, es decir, la NSA mantiene una conexión directa con los servidores de grandes proveedores como: Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL, Apple.

7National Security Agency. (2013). PRISM/US-984XN Overview: The SIGAD Used Most in NSA Reporting. 21/10/2013, de Le Monde Sitio web: https://goo.gl/fAJ38O

Inclusive en una de las láminas filtradas (PRISM/US-984XN Overview: The SIGAD Used Most in NSA Reporting), se nos presenta un costo aproximado del proyecto, el cual ronda los 20 millones de dólares por año y los años en los que los proveedores de servicio fueron agregados al proyecto.

Participación en empresas de seguridad

Otra técnica utilizada por la NSA para incrementar su poder de intercepción de señales, es generar acuerdos con empresas productoras de equipos de seguridad. En dichos acuerdos, los equipos funcionan normalmente, pero antes de salir al mercado, son alterados para poder ser habilitados en modo espía (SIGINT mode). *Computer Network Operations SIGINT Enabling* [8]

En dicho artículo se revela el total de presupuesto informal asignado para incluir dichos cambios en el software de los equipos de seguridad. La siguiente tabla habla del presupuesto de 254.9 millones de dólares para el año 2013 y su comparativa con los años 2012 y 2011.

This Exhibit is SECRET//NOFORN									
	FY 2011[1] Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding ($M)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—
[1]Includes enacted OCO funding.							Totals may not add due to rounding.		

Influencia en creación de estándares

La influencia en la adopción de estándares de seguridad, protocolos y productos, es un objetivo importante en la política de seguridad de Estados Unidos de

8National Security Agency. (2012). Computer Network Operations SIGINT Enabling. 28/11/2016, de The Guardian Sitio web: https://goo.gl/tmNv3E

América. En su plan de objetivos del 2012-2016[9], podemos observar a partir del punto 2.1.4 al 2.2 que citan lo siguiente:

> 2.1.4. (TS//SI//REL) Influence the global commercial encryption market through commercial
> relationships, HUMINT, and second and third party partners
> 2.1.5. (S//SI//REL) Continue to invest in the industrial base and drive the state of the art for High Performance Computing to maintain pre-eminent cryptanalytic capability for the nation
> 2.2. (TS//SI//REL) Defeat adversary cybersecurity practices in order to acquire the SIGINT data we need from anyone, anytime, anywhere

Básicamente los puntos anteriores significan que utilizarán los medios posibles a su alcance para influenciar el mercado de encripción, elevar su capacidad de encripción dentro de EEUU y, finalmente, detener cualquier práctica de seguridad de la información para mantener la captura de información de cualquiera, donde se requiera y en cuándo sea.

Obtención de información de fuentes abiertas (OSINT)

La obtención de información también se realiza a través de fuentes públicas, como se le conocen, fuentes abiertas. Según el artículo *OSINT Fusion Project*[10], las fuentes tradicionales de OSINT, provienen primordialmente de: noticieros, resúmenes recuperados, información de fabricantes. Dicha información es útil para entender el contexto de diversas situaciones, obtener algunos análisis de ataques y vulnerabilidades, sin embargo, la información puede ser vieja o de segunda mano, así como puede no contener el detalle necesario.

En cuestiones de vigilancia, existe mucha información personal en fuentes abiertas y, aunque la NSA no contara con el proyecto PRISM, podría echar mano de varias

9National Security Agency. (2012). SIGINT Strategy. 28/11/2016, de The New York Times Sitio web: https://goo.gl/rGDOVk
10Lockheed Martin IS&GS Intelligence. (2009). OSINT Fusion Project. 28/11/2016, de The Intercept Sitio web: https://goo.gl/lqpcQd

herramientas públicas para obtener la información disponible en fuentes abiertas. Así lo demuestra el Documento *Open Source for Cyber Defense / Progress*[11] en donde se presenta una lista de las herramientas que el gobierno de Estados Unidos de América sugiere para la obtención de información abierta. Me permito traducir parte de la tabla para un mayor entendimiento.

Fuente de la información	Naturaleza de la información
alexa.com	Lista de dominios populares, ha sido utilizada para encontrar redes sociales extranjeras para apoyar en el análisis en investigaciones.
user-agents.org	Buscador de user-agents, es decir, identificadores de programas clientes no comunes, útil para encontrar entradas maliciosas a sistemas.
www.nsrl.nist.gov	Acceso a hashes conocidos de archivos COTS
www.maxmind.com (lista ASN)	Usado para mapear los segmentos de IPs de redes que están siendo monitoreadas.
ZeusTracker.abuse.ch	Rastreador de malware Zeus, incluye IPs, binarios y dominios. A utilizarse por el equipo e-crimen.

11Government Communications Headquarters. (2012). Open Source for Cyber Defence / Progress. 5/12/2016, de The Intercept Sitio web: https://goo.gl/WKakS7

Existen otras muchas herramientas más sofisticadas que las ya mencionadas, éstas son abiertas, o bien, requieren un pequeño pago para su uso. El verdadero valor de las fuentes abiertas radica en la conducta de los usuarios de servicios gratuitos en Internet, quienes aportan grandes cantidades de información sobre sus hábitos, gustos, deseos y pensamientos, lo que hace más sencillo la recopilación de información con fines de espionaje.

3. Almacenamiento de la información

Entre varios esfuerzos de almacenamiento de metadatos, el proyecto TEMPORA, es el más interesante. Dicho sistema puede retener temporalmente, según el documento original, tres días la información completa y treinta días de metadatos de cualquier usuario de Internet y telefonía, aunque el mismo individuo no se encuentre bajo investigación. [12]

Según la misma NSA[13], en uno de sus documentos revelados, se generan diariamente 1,826 petabytes de información diariamente, de ellos, son utilizados el 1.6% (29.21 petabytes). El artículo de *The Guardian* señala que, la información podría ser almacenada hasta por 30 días[14], lo que nos entregaría un total de 876.48 petabytes de espacio de almacenamiento requerido.

Realizando una estimación básica del costo de un sistema de almacenamiento de 1PB por $ 375,000 dólares, la inversión realizada por EEUU en el sistema de almacenamiento de 30 días, es aproximada a los $ 328 millones de dólares. Este presupuesto es únicamente de la inversión inicial del equipo, para mantener operando dichos sistemas, son necesarios adicionalmente: Ingenieros, Datacenters (edificios para resguardar equipo electrónico), aires acondicionados, sistemas contra incendio y, por si fuera poco, un intenso consumo de energía eléctrica.

Fuentes sin confirmar, sugieren que la capacidad de almacenamiento ya es tan alta (entre 3 y 12 exabytes), que pueden guardar todos los metadatos generados sin borrarlos, en realidad, no existe una confirmación sobre lo anterior, pero es importante comprender que nuestra actividad electrónica está generando una huella que no desaparecerá inmediatamente. Nuestros hábitos electrónicos están lejos de ser efímeros.

12Government Communications Headquarters (GCHQ). (2012). TEMPORA. 18/06/2014, de Der Spiegel Sitio web: https://goo.gl/qRaIzX.
13National Security Agency. (2013). The National Security Agency: Missions, Authorities, Oversight and Partnerships. 22/10/2016, de National Security Agency Sitio web: https://goo.gl/2dxzqJ
14James Ball. (2013). NSA stores metadata of millions of web users for up to a year, secret files show. 22/10/2016, de The Guardian Sitio web: https://goo.gl/cyjyIu

4. Interpretación de los metadatos

La interpretación de la información interceptada es primordial para lograr sus objetivos, de otro modo, EEUU acabaría con toneladas de información que no puede ser evaluada. Según el artículo *SKYNET: Applying Advanced Cloud-based Behavior Analytics*[15], el proyecto SKYNET combina una serie de complejos cruces geoespaciales, geotemporales, patrones de vida y análisis de viaje, para convertir información cruda a patrones de actividad sospechosa.

El análisis de la información puede realizarse de dos formas: la primera es bajo demanda y la segunda por análisis automático. En la primera, se pueden realizar preguntas bajo demanda como:

- ¿Quién fue de un pueblo A al pueblo B y pasó por pueblo C dos veces ésta semana?
- ¿A quién llamó la persona que cumplió con ese patrón de viaje?
- ¿Quién apaga el equipo frecuentemente?
- ¿Quién cambia el chip SIM frecuentemente?

En la segunda opción, el sistema busca patrones especiales poniendo atención a los siguientes puntos:

- Itinerarios de viaje
- Visitas regulares
- Sólo recepción de llamadas
- Cambio excesivo de chip SIM o teléfono
- Apagado frecuente del dispositivo
- Viajes en días específicos de la semana
- Acompañantes de viaje
- Patrones similares de viaje
- Contactos en común
- Visitas a aeropuertos
- Visitas al extranjero
- Viajes nocturnos
- Movimiento permanente

La gráfica del mismo artículo, nos muestra los patrones de viaje y los equipos involucrados en el mismo. *SMARTTRACKER Travel View*.

15National Security Agency. (2012). SKYNET: Applying Advanced Cloud-based Behavior Analytics. 28/11/2016, de The Intercept Sitio web: https://goo.gl/JwjO0E

Este tipo de tecnología de reconocimiento de patrones en hábitos de uso de celulares, es igualmente viable para uso de computadoras y los patrones de navegación en Internet. Ésta es una pequeña muestra de lo que es posible lograr con análisis de BigData.

El análisis de estos datos, en teoría, tiene como finalidad disuadir actividades terroristas, empero, puede utilizarse para dispersar grupos disidentes, activistas políticos y para coadyuvar a cualquier otro tipo de interés que los operadores de la maquinaria tengan.

5. Implicaciones

A raíz de las filtraciones realizadas, la relación de los usuarios, ciudadanos americanos y del resto del mundo, con Internet, se modificó en varios aspectos. Cubriré algunos dividiéndolos en: económicos, políticos y técnicos.

Económicas

Según el artículo *Surveillance Costs: The NSA's Impact on the economy, Internet Freedom & cybersecurity*[16] las pérdidas económicas pueden deberse a dos factores principalmente: Desconfianza de los mercados a las soluciones americanas y Nuevas regulaciones de gobiernos que busquen evitar el espionaje americano.

La desconfianza en soluciones americanas ha crecido, los mercados más vulnerables son los servicios ofrecidos bajo demanda o en la nube. En donde la información de los usuarios permanece hospedado en servidores probablemente americanos y, por ende, sujetos al escrutinio de las agencias de seguridad.

Varios países como el alemán o el brasileño, reaccionaron inmediatamente a las revelaciones, condenándolas. Es de esperarse que algunos gobiernos, tanto de esos países como del resto del mundo, comiencen a tomar en serio la seguridad de su información en Internet, dando como resultado una inversión brutal en infraestructura y comunicaciones propias; muy posiblemente, desarrollando equipo o soluciones que no estén obligadas a ser escrutadas por la NSA.

Actualmente no se cuenta con un estimado de pérdidas o ganancias económicas de empresas americanas derivadas de las revelaciones, lo anterior debido a la secrecía con la que los tomadores de decisiones se conducen en éste ámbito, sin embargo, según Daniel Castro, analista de tecnologías de la información, en el artículo

16Robyn Greene, et al.. (2014). Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity. 6/12/2016, de New America Sitio web: https://goo.gl/BsoFXn

Revelations of N.S.A. Spying Cost U.S. Tech Companies[17] en *The New York Times*, comenta que las pérdidas podrían ascender a **35 mil millones de dólares** en servicios en la nube. Otras pérdidas no cuantificables están relacionadas con los concursos comerciales, públicos o privados, donde las empresas americanas ya no son invitadas, o bien, contratos de largo plazo que aún no vencen para su renovación.

De cualquier manera, las revelaciones de Snowden cambiaron la manera en la que se invertía en seguridad informática, algunos jugadores clásicos del mercado perderán, otros que ofrezcan un grado mayor de secrecía, ganarán. Indudablemente, la inversión en seguridad informática aumentará de forma considerable durante las próximas décadas.

Políticas

Hasta hace una década, las zonas de influencia de EEUU estaban muy bien demarcadas en la colectividad, podría realizarse una encuesta sobre la postura que EEUU tomaría tras alguna acción bélica internacional y, en su mayoría, se podría acertar en la predicción, sin embargo, en los últimos años vimos cómo Crimea y Sebastopol fueron anexados a la federación rusa sin ninguna repercusión; también fuimos testigos de los primeros indicios de reconciliación entre EEUU y el gobierno cubano.

La tendencia mundial contra el neoliberalismo cambió el panorama político de occidente, la votación a favor de la salida de Gran Bretaña de la Unión Europea (Brexit) y la elección de Donald Trump como presidente de EEUU, con el objetivo de la ruptura de tratados internacionales sostenidos con México, crean la suficiente incertidumbre para cuestionarse la estabilidad de antiguos bloques geopolíticos (OTAN).
Las filtraciones de Edward Snowden, no son un parteaguas político en sí mismas, pero sí una pieza de un rompecabezas mayor, tal vez, el aderezo perfecto para esta ensalada de cambios; un elemento desestabilizante para los planes establecidos.

17CLAIRE CAIN MILLER. (2014). Revelations of N.S.A. Spying Cost U.S. Tech Companies. 06/12/2014, de The New York Times Sitio web: https://goo.gl/Xot3I4

En este instante en el que estoy escribiendo el ensayo, varios analistas políticos internacionales coinciden en una sola cosa: No es posible predecir la política internacional que seguirá Donald Trump hasta que inicie su mandato. Por lo tanto, me abstendré de hacer predicciones que, sin poder sustentarlas con hechos, se mantendrían como meras especulaciones, empero, la certidumbre y confianza que sus aliados le demandan a EEUU, hoy se encuentra en entredicho.

Quiero cerrar este apartado político citando lo expuesto en el artículo *Implications of NSA Revelations on US Foreign Policy*[18]:

> "A large part of America's power has come not from its military or economic strength, but from the perception that while America might do the wrong thing, it will do so for the right reasons. Revelations such as these weaken that belief."

> "Gran parte del poder de EEUU proviene, no de su milicia o fortaleza económica, sino de la percepción de que EEUU puede cometer actos incorrectos justificados por las razones correctas. Las revelaciones como éstas debilitan esas creencias."

Técnicas

Una de las características intrínsecas de las tecnologías de la información y sistemas, es la mejora continua, tanto como elemento que aporta valor a la venta de productos y servicios, como elemento necesario para mantener la información protegida. Las filtraciones de espionaje en Internet de la NSA, se presentan como un catalizador de la innovación, dejando ver que es imperante nunca dar por sentado algún grado de conformidad con el *status quo*.

Dicho de otro modo, es fundamental elevar el nivel de los estándares de seguridad existentes en todas las comunicaciones, empero, los organismos y empresas que por

18Xenia Wickett. (2013). Implications of NSA Revelations on US Foreign Policy. 06/12/2016, de Chatham House, The Royal Institute of International Affairs Sitio web: https://goo.gl/r0RbhR

naturaleza serían las encargadas de dictar los estándares, se encuentran atadas de manos al ser americanas o encontrarse físicamente en EEUU.

Trasladar la responsabilidad de la emisión de estándares de seguridad del gobierno de EEUU a otro gobierno, sería simplemente cambiar al jugador en turno y levantaría una discusión sobre la autoridad moral del nuevo árbitro.

Por otro lado, la generación de un estándar de facto por medio de una organización privada, es poco viable debido a la gran disparidad de poder económico entre las transnacionales americanas y los posibles contendientes chinos, rusos o europeos.
Los nuevos jugadores deberán de invertir, tanto en servicios alternativos a los americanos, como en las capas más bajas de aplicación y hardware. A continuación enlisto algunos puntos que, deberán ponerse en tela de juicio, como lo comentan en *Extra-PRG Meeting on the Technical Implications of the NSA and GCHQ Revelations*[19]:

1. Microcontroladores y chips de comunicación fabricados en EEUU.
2. Algoritmos de encripción.
3. Secure Sockets Layer (SSL)
4. Chips con algoritmos defectuosos para generación de números aleatorios.
5. Entidades certificadoras falsas. (certificados de seguridad para sitios en Internet)
6. Personal encubierto de la NSA trabajando dentro de organizaciones.
7. Enlaces de comunicación de alta velocidad entre regiones.
8. Equipo de telecomunicaciones con puertas traseras.
9. Aplicaciones móviles, sistemas operativos y servicios brindados en la nube por empresas americanas.
10. Equipos de cómputo, celulares y tabletas.

Mikko Hypponen en su participación en *TED talks*[20], aborda estos problemas de forma similar y, aunque la creación de un ecosistema libre de intrusión es viable, la inversión económica y en mano de obra, sería titánica. Para sufragar estas necesidades, será necesario abordar el problema desde una óptica diferente: El software libre.

19Seda, et al.. (2013). Extra-PRG Meeting on the Technical Implications of the NSA and GCHQ Revelations. 06/12/2016, de New York University's Information Law Institute Sitio web: https://goo.gl/I4Zw2F
20Mikko Hypponen. (2013). How the NSA betrayed the world's trust — time to act. 06/12/2016, de TED Ideas worth spreading Sitio web: https://goo.gl/bsknuX

El software libre busca preservar cuatro derechos fundamentales del usuario[21]:

1. Libertad de uso
2. Libertad para cambiar el software
3. Libertad para compartir el software
4. Libertad para compartir los cambios

La única manera que tiene el software libre para mantener dichas libertades, es la obligación de compartir el código fuente del mismo, ergo, la receta con la que el software se realizó. Esto es muy importante porque al compartir el código fuente, muchos individuos y organizaciones a nivel mundial pueden revisar si existen errores, brechas de seguridad y puertas traseras.

Adicionalmente, tener el código abierto, facilita un esquema colaborativo, ya que el resultado, a la vista de todos, logra conjuntar los esfuerzos de varios grupos interesados en la misma herramienta, los cuales, pueden o no, pertenecer a los mismos países u organizaciones.

Lo mismo ocurre con la inversión económica, mientras que para una única empresa, mantener la nómina de cien personas trabajando en un desarrollo de seguridad, le resulta oneroso; para diez empresas, mantener una nómina de diez personas trabajando en el mismo desarrollo, les resultará más asequible.

No todo es miel sobre hojuelas, uno de los factores de éxito de estos proyectos abiertos, será conciliar los intereses de las organizaciones patrocinadoras para evitar los llamados *forks* o derivaciones que podrían pulverizar los esfuerzos.

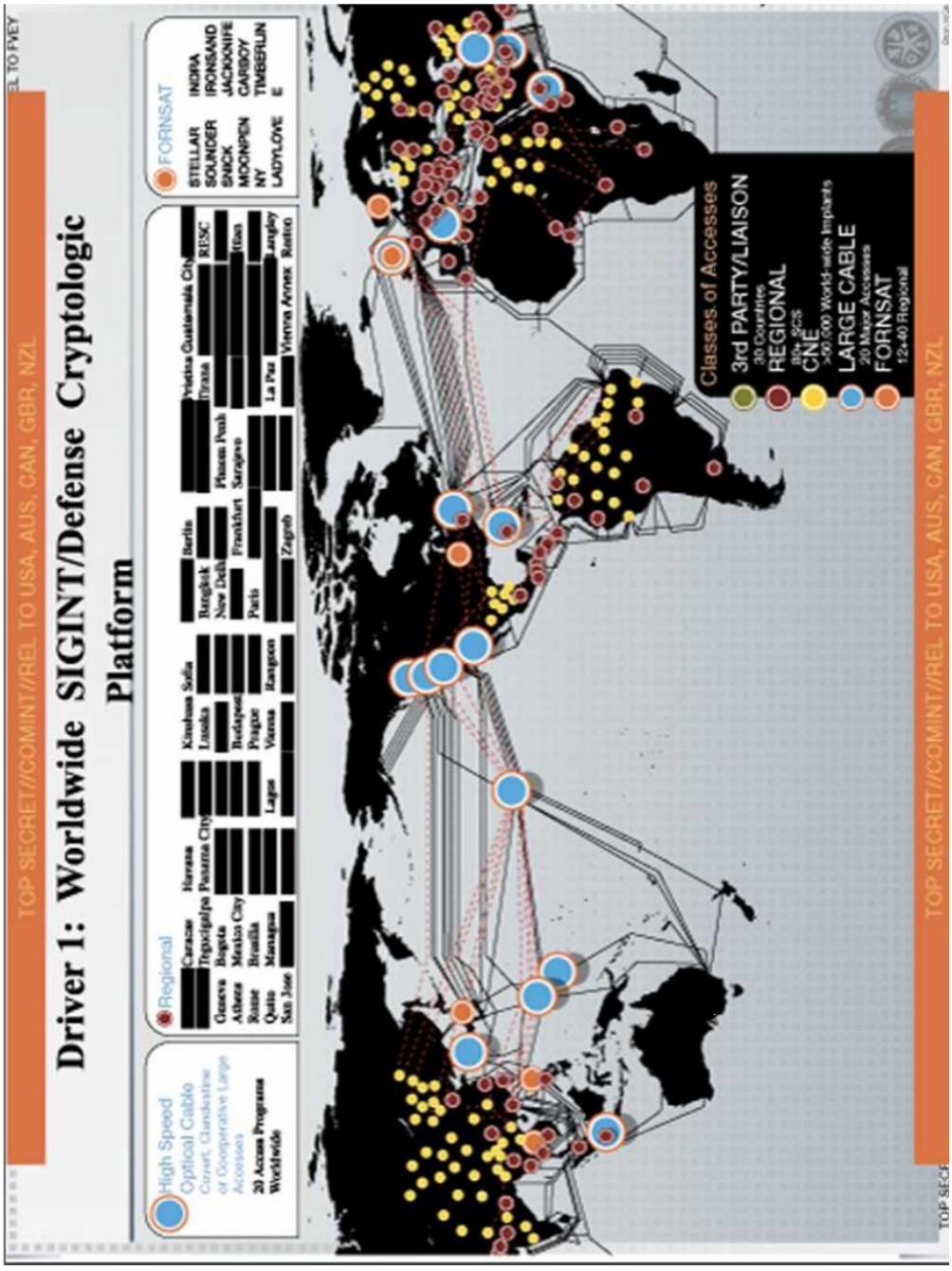
21FSF. (NA). What is free software?. 09/12/2016, de Free Software Foundation Sitio web: https://goo.gl/xQQrbF

6. Conclusión

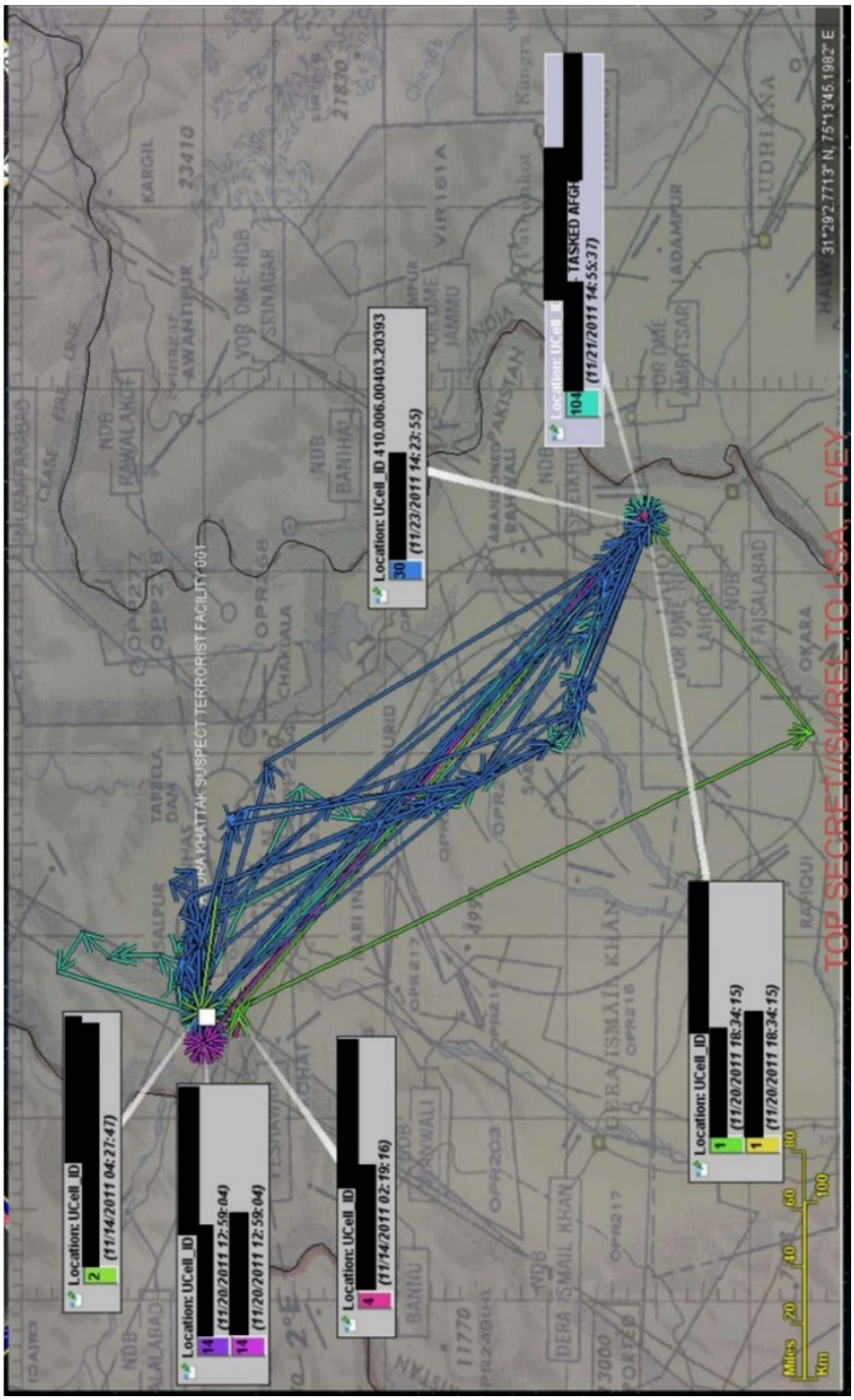
Las técnicas de espionaje han existido desde el inicio de las guerras, en el antiguo testamento encontramos la existencia de Rahab, una prostituta que dio asilo a espías para la toma de Jericó. Las revelaciones de Edward Snowden, ex-consultor de la NSA, nos hicieron recordar que el Internet no es más el lugar idílico de acceso democrático a la información, es, en verdad, una extensión de la realidad humana en donde se espiará y se combatirá como en cualquier otro sitio.

7. Imágenes

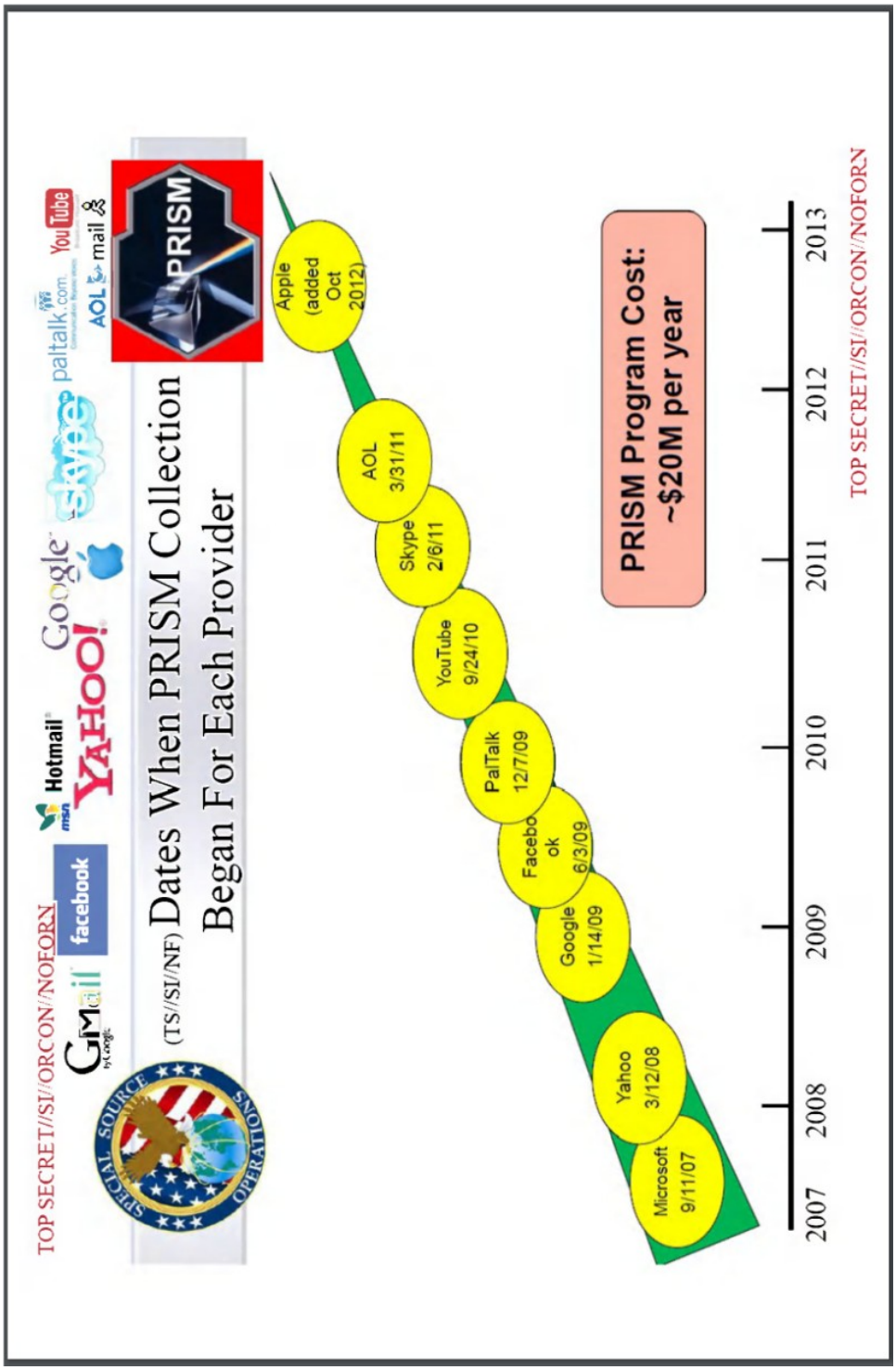
Driver 1: Worldwide SIGINT/Defense Cryptologic Platform



SMARTTRACKER Travel View



PRISM/US-984XN Overview: The SIGAD Used Most in NSA Reporting



Bibliografía

La mayoría de la información se localizó gracias al sitio: *Snowden Digital Surveillance Archive (https://snowdenarchive.cjfe.org)*, un sitio en Internet dedicado a catalogar los documentos clasificados filtrados por Edward Snowden, gracias al esfuerzo del grupo *Canadian Journalists for Free Expression (CJFE).*

- Department of the Army. (2004). Signals Intelligence. 2016, de Department of the Army Sitio web: http://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap8.htm
- National Security Agency. (2012). Driver 1: Worldwide SIGINT/Defense Cryptologic Platform. 23/11/2013, de NRC Sitio web: https://goo.gl/CQKQ18
- National Security Agency. (2007). US, German SIGINTers Increase Cooperation on African Targets. 18/06/2014, de Der Spiegel Sitio web: https://goo.gl/IQf5u6
- National Security Agency. (2013). NSA Intelligence Relationship with Israel. 03/08/2014, de The Intercept Sitio web: https://goo.gl/tLp25t
- Government Communications Headquarters (GCHQ). (2012). TEMPORA. 18/06/2014, de Der Spiegel Sitio web: https://goo.gl/qRaIzX
- James Ball. (2013). NSA stores metadata of millions of web users for up to a year, secret files show. 22/10/2016, de The Guardian Sitio web: https://goo.gl/cyjyIu
- National Security Agency. (2013). The National Security Agency: Missions, Authorities, Oversight and Partnerships. 22/10/2016, de National Security Agency Sitio web: https://goo.gl/2dxzqJ
- BRUCE SCHNEIER. (2014). Everything We Know About How the NSA Tracks People's Physical Location. 23/11/2016, de The Atlantic Sitio web: https://goo.gl/Jh82sy
- David Adrian, et al.. (2015). Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. 28/11/2016, de WeakDH.org Sitio web: https://goo.gl/gvKQ4J
- National Security Agency. (2012). SIGINT Strategy. 28/11/2016, de The New York Times Sitio web: https://goo.gl/rGDOVk
- National Security Agency. (2013). PRISM/US-984XN Overview: The SIGAD Used Most in NSA Reporting. 21/10/2013, de Le Monde Sitio web: https://goo.gl/fAJ38O
- Government Communications Headquarters. (2012). Open Source for Cyber Defence / Progress. 5/12/2016, de The Intercept Sitio web: https://goo.gl/WKakS7
- Robyn Greene, et al.. (2014). Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity. 6/12/2016, de New America Sitio web: https://goo.gl/BsoFXn
- CLAIRE CAIN MILLER. (2014). Revelations of N.S.A. Spying Cost U.S. Tech Companies. 06/12/2014, de The New York Times Sitio web: https://goo.gl/Xot3I4

- Xenia Wickett. (2013). Implications of NSA Revelations on US Foreign Policy. 06/12/2016, de Chatham House, The Royal Institute of International Affairs Sitio web: https://goo.gl/r0RbhR
- Mikko Hypponen. (2013). How the NSA betrayed the world's trust — time to act. 06/12/2016, de TED Ideas worth spreading Sitio web: https://goo.gl/bsknuX
- Seda, et al.. (2013). Extra-PRG Meeting on the Technical Implications of the NSA and GCHQ Revelations. 06/12/2016, de New York University's Information Law Institute Sitio web: https://goo.gl/I4Zw2F
- FSF. (NA). What is free software?. 09/12/2016, de Free Software Foundation Sitio web: https://goo.gl/xQQrbF