PROGRAMAS DE VIGILANCIA DE INTERNET

TRABAJO DE FIN DE MÁSTER

MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES (MISTIC)

Autor: Santiago Martín López

Directora: Cristina Pérez Solà

Centro: Universitat Oberta de Catalunya

Fecha: 20 de Junio de 2014

Agradecimientos

A Ana, mi mujer, por todo el cariño, el apoyo y la comprensión que he recibido de ella en la realización de este Máster

RESUMEN

Las revelaciones realizadas en el año 2013 por Edward Snowden, antiguo empleado de la Agencia Nacional de Seguridad de Estados Unidos (NSA), nos muestran un listado de programas informáticos diseñados para recopilar, almacenar y tratar enormes cantidades de información que viajan por internet. En el trabajo realizaremos un resumen de las revelaciones de Snowden, destacando los momentos más relevantes y analizaremos por qué se producen en ese momento. Basándonos en las revelaciones comprobaremos que existe el conocimiento y apoyo de estos programas de vigilancia por parte de muchos gobiernos, al igual que por grandes empresas tecnológicas, que ponen en peligro la privacidad de las comunicaciones a nivel mundial. Desde esta perspectiva, analizaremos la historia de los diferentes programas de vigilancia masiva en internet, así como su funcionamiento. En base a este análisis, mostraremos las medidas y herramientas que pueden adoptar los ciudadanos para mantener la privacidad de sus comunicaciones a través de Internet.

Palabras clave: Internet, vigilancia, programas, Snowden, NSA, revelaciones, privacidad.

Área del proyecto: Seguridad en Servicios y Aplicaciones. Privacidad

ABSTRACT

The revelations made in 2013 by Edward Snowden, former employee of the National Security Agency of the United States (NSA), show us a list of computer programs designed to collect, store and treat huge amounts of information travelling through the Internet. In this work we will summarize Snowden's revelations, highlighting the most relevant moments and we will analyze why those revelations occur in that moment. Basing on those revelations we will prove these surveillance programs, which put in hazard communication privacy at a worldwide level, are known and supported by many governments, as well as by big technology companies. From this perspective, we will analyze the history of the different massive surveillance programs in Internet, as well as their operation. Basing on this analysis, we will show the measures and tools citizens can adopt in order to maintain privacy in their communications through Internet.

Keywords: Internet, surveillance, programs, Snowden, NSA, revelations, privacy.

Project Area: Security in Services and Applications. Privacy

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

1. PLAN DE TRABAJO

a) Introducción

Basamos nuestro trabajo en las revelaciones realizadas en el año 2013 por Edward Snowden, antiguo empleado de la Agencia Nacional de Seguridad (NSA) estadounidense, a los periódicos *The Guardian* y *The Washington Post*, en las que nos da a conocer una serie de programas informáticos que recogen y almacenan todo tipo de información que viaja a través de Internet de manera masiva. Estos programas apoyados por otros gobiernos y grandes empresas, ponen en peligro la privacidad de los datos y las comunicaciones de los ciudadanos a nivel mundial, más aún cuándo han sido incluso respaldadas por leyes estadounidenses y no estadounidenses.

b) Objetivos del Trabajo de Fin de Máster

Los objetivos de este proyecto son:

- Crear un informe actualizado de los programas de vigilancia de Internet actuales. El informe revisará los programas de vigilancia de conocimiento público (actuales) e investigará los antecedentes históricos y contextuales que permiten a estos programas aparecer y ser revelados al público.
- Estudiar las posibles medidas y las herramientas que pueden utilizar los ciudadanos para mantener su privacidad cuando se transmite información digitalmente.

c) La descripción de la metodología que se seguirá durante el desarrollo del TFM.

Para desarrollar el Trabajo de Fin de Máster utilizaremos una **metodología en cascada**, siguiendo una lista de tareas que dependen una de otra:

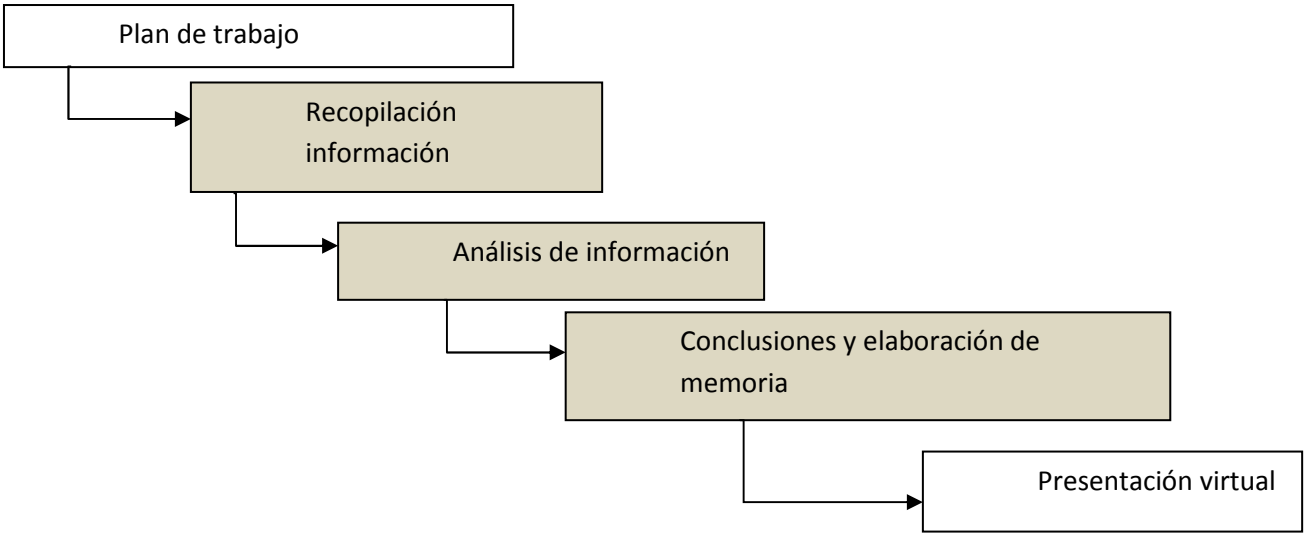

Figura 1. Esquema metodología en cascada

La metodología en cascada utilizada está compuesta por dos iteraciones (los componentes están sombreados), una para cada parte del Trabajo de Fin de Máster (PEC2 y PEC3) en las que se recopila, analiza y se saca conclusiones al respecto.

d) El listado de las tareas a realizar para alcanzar los objetivos descritos.

El listado de las tareas viene marcado por las fechas límite de las entregas del Trabajo de Fin de Máster. El inicio del Trabajo es el 26/02/2014, fecha de inicio de la asignatura, mientras que el plazo máximo establecido para entregar la memoria y la presentación virtual es el 20/06/2014:

TAREAS	FECHA LÍMITE
PEC1- Elaboración de un plan de trabajo	17/03/2014
PEC2- Informe de los programas de vigilancia en Internet.	21/04/2014
PEC3- Estudio de medidas y herramientas para mantener la privacidad	30/05/2014
PEC4- Entrega de memoria y producto resultante	13/06/2014
Entrega de la Presentación virtual	20/06/2014

Figura 2. Listado de tareas a realizar con sus fechas límite

e) La planificación temporal detallada de estas tareas y sus dependencias.

Para generar la planificación del Trabajo de Fin de Máster hemos utilizado la herramienta Open Source *Gantt Project*.

Hemos desglosado las diferentes PEC en tareas para mostrar los distintos pasos que tenemos que seguir para desarrollar el Trabajo de Fin de Máster. La tabla de hitos resultante es la siguiente:

Nombre	Fecha de inicio	Fecha de fin
PEC 1 - Plan de trabajo	26/02/14	17/03/14
Descripción del problema	26/02/14	27/02/14
Objetivos del TFM	28/02/14	1/03/14
Definición de la metodología	2/03/14	4/03/14
Listado de tareas	5/03/14	7/03/14
Planificación temporal	8/03/14	12/03/14
Revisión del estado del arte	13/03/14	17/03/14
PEC 2 - Programas de vigilancia de internet	18/03/14	21/04/14
Recopilación de información	18/03/14	27/03/14
Análisis de información recogida	28/03/14	8/04/14
Elaboración primera parte de la memoria	9/04/14	21/04/14
PEC 3 - Estudio y herramientas para mantener la privacidad	22/04/14	30/05/14
Recopilación de información	22/04/14	2/05/14
Análisis de información recogida	3/05/14	19/05/14
Elaboración segunda parte de la memoria	20/05/14	30/05/14
PEC 4 - Entrega de memoria y producto resultante	31/05/14	13/06/14
Elaboración final de la memoria	31/05/14	13/06/14
Entrega de la Presentación Virtual	14/06/14	20/06/14
Elaboración de la Presentación Virtual	14/06/14	20/06/14

Figura 3. Tabla de hitos

Mostramos gráficamente la planificación temporal mediante el siguiente diagrama de Gantt:

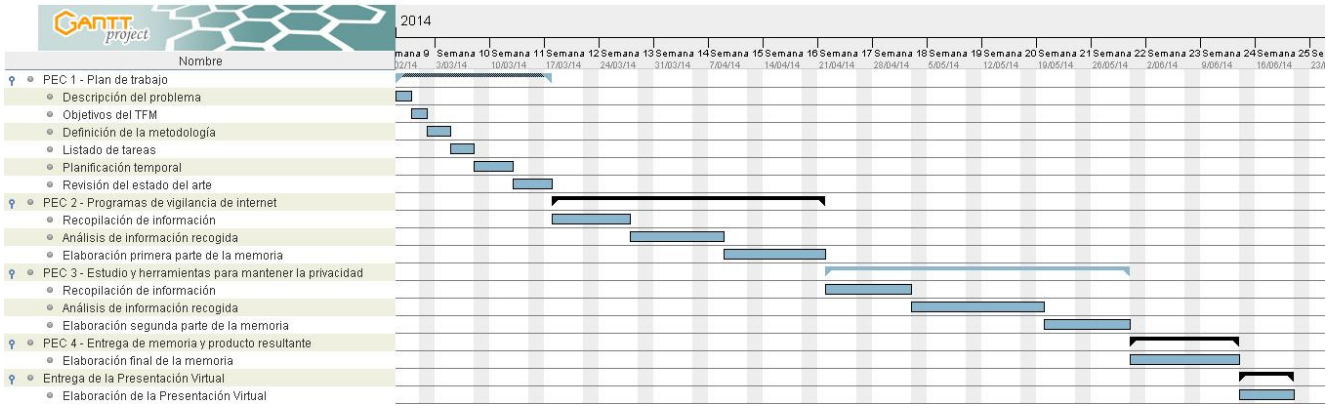

Figura 4. Diagrama de Gantt

f) Una pequeña revisión del estado del arte.

En la primera parte del Trabajo de Fin de Máster, elaboraremos un informe investigando los antecedentes históricos y contextuales que permiten aparecer a los programas de vigilancia, y posteriormente cómo se dan a conocer públicamente, enlazando con un análisis de los programas actuales.

1. Antecedentes históricos
    a. Segunda Guerra Mundial y los orígenes de los tratados Reino Unido – Estados Unidos
    b. ECHELON : Nexo de vigilancia de comunicaciones entre Reino Unido – Estados Unidos
    c. 1975 -1978: Watergate y la comisión Church
    d. Contexto después del 11 de Septiembre: ampliación de las competencias de inteligencia
2. Actualidad: Revelaciones de Edward Snowden
    a. Breve historia de las filtraciones de Edward Snowden
    b. ¿Por qué se realizan las revelaciones de Snowden en este momento?
    c. Conocimiento de otros países sobre los programas de vigilancia de Internet
    d. Colaboración de grandes empresas con las agencias de seguridad e inteligencia
3. Programas de vigilancia actuales conocidos después de las revelaciones de Snowden
    a. PRISM
    b. Tempora
    c. Upstream
    d. XKeyScore
    e. BULLRUN

En la segunda parte de la memoria del Trabajo de Fin de Máster, realizaremos un análisis de las medidas y de las herramientas digitales que tienen a su disposición los ciudadanos para contrarrestar la acción de los programas de vigilancia.

4. Medidas de protección frente a los programas de vigilancia
    a. Cifrar las comunicaciones
    b. Uso de protocolos de comunicación seguros

c. Anonimato y privacidad en la red: Tor

d. Motores de búsqueda de Internet

e. Privacidad en las llamadas telefónicas por Internet: Cifrar VoIP

2. ANTECEDENTES HISTÓRICOS

Analizar los programas y los sistemas de vigilancia electrónica que se han ido utilizando a lo largo de la historia y cuyo origen se remonta a la Segunda Guerra Mundial nos servirá de base para comprender la situación actual de la vigilancia masiva por Internet.

a) Segunda Guerra Mundial y los orígenes de los tratados Reino Unido – Estados Unidos

Los orígenes de los tratados Reino Unido – Estados Unidos en materia de inteligencia nacieron a partir de la estrecha colaboración que mantuvieron ambos países durante la Segunda Guerra Mundial, en particular por el trabajo realizado para descifrar los códigos alemanes y japoneses. Dicha colaboración se tradujo en mejoras tecnológicas para romper códigos de encriptación (creación de *Colossus*, primera computadora electrónica digital).

De esta experiencia surgió el primer acuerdo en materia de inteligencia, llamado BRUSA que derivó más tarde en UKUSA (United Kingdom-United States Security Agreement; Tratado de seguridad entre el Reino Unido y los Estados Unidos), la alianza para compartir información de inteligencia formada en marzo de 1946. Es ahí donde tienen origen el GCHQ (Cuartel General de Comunicaciones del Gobierno Británico) y la NSA (Agencia Nacional de Seguridad estadounidense), creada en secreto en 1952, por el presidente Harry S. Truman.

Aunque la alianza entre el GCHQ y la NSA surge nada más empezar la Guerra Fría, posteriormente fue abierta a tres países: Australia, Canadá y Nueva Zelanda, para formar el grupo denominado “Cinco Ojos”, que ayudaron a hacer posible la interceptación de comunicaciones por todo el mundo.

Los detalles del acuerdo inicial UKUSA fueron mantenidos en secreto durante décadas, hasta que ambos países los hicieron públicos en 2010.

b) ECHELON: Nexo de vigilancia de comunicaciones entre Reino Unido – Estados Unidos

Echelon es un sistema informático. La red *Echelon* es un entramado de antenas, estaciones de escucha, radares y satélites apoyados por submarinos y aviones espías, concebidos para interceptar las comunicaciones mundiales, para luchar contra el terrorismo y el tráfico de drogas.

El nacimiento de la red Echelon se produjo en 1977, cuando sus satélites consiguieron interceptar información de las redes de satélites Inmarsart (red de satélites de comunicaciones entre embarcaciones) e Intelsat (red de satélites de telecomunicaciones).

Estados Unidos y Gran Bretaña han negado la existencia de Echelon, pero entre 1998 y 1999, el especialista en inteligencia Jeff Richelson, obtuvo una serie de documentos de la Marina y de la Fuerza Aérea de los EEUU, en los que se hacía referencia a la existencia continuada, la escala y la expansión del sistema Echelon.

El potencial de la red Echelon es muy grande. Se puede interceptar toda clase de señales electrónicas y de comunicaciones por radio y por satélites, incluyendo las comunicaciones por voz. Una vez que detecta una comunicación que contiene palabras clave o ciertas combinaciones de estas (buscando patrones específicos en cada comunicación), el sistema las monitorea y graba, etiquetándolas y enviándolas a distintos centros para su procesamiento, que se encargarán de descifrar y traducir su contenido que posteriormente quedará almacenado.

c) 1975 -1978: Watergate y la comisión Church

El caso Watergate nació en 1972 con el arresto de cinco hombres que se habían encargado de espiar al Comité Nacional Demócrata en el complejo de oficinas Watergate de Washington. Dos periodistas del *Washington Post*, Carl Bernstein y Bob Woodward, investigaron durante dos años este hecho, reuniendo pruebas suficientes que apuntaban al presidente Richard Nixon y a su entorno. En una investigación posterior del Senado se reveló que Nixon tenía un sistema de grabación de cintas magnéticas en sus oficinas y que se habían grabado gran cantidad de conversaciones incluso dentro de la Casa Blanca, las que, en un principio, se negó a entregar. Todo ello llevó a la dimisión de Nixon en 1974.

Las revelaciones de la prensa por el caso Watergate llevaron al Senado a crear el "Comité Selecto del Senado de los Estados Unidos para el Estudio de las Operaciones Gubernamentales respecto a las Actividades de Inteligencia", presidido por el Senador Frank Church, que investigó las sospechas existentes sobre los abusos que los servicios de inteligencia y seguridad habían realizado en la Oficina del Presidente de los Estados Unidos.

Como resultado de estas investigaciones, en 1978 se creó la FISA (Foreign Intelligence Surveillance Act of 1978 – Ley de Vigilancia de la Inteligencia Extranjera de 1978), ya que en el caso Watergate se había violado la Cuarta Enmienda de la Constitución, que protege el derecho a la privacidad y el derecho a no sufrir una invasión arbitraria. Dicha ley establece una supervisión judicial y del Congreso de las actividades de vigilancia a entidades y personas extranjeras en Estados Unidos. De esta manera, se permite la vigilancia a personas extranjeras, y si hubiera una persona estadounidense involucrada en la vigilancia, se requeriría una autorización judicial.

d) Contexto después del 11 de Septiembre: ampliación de las competencias de inteligencia

El Senado de los Estados Unidos legitimó la práctica de escuchas telefónicas a partir de los ataques terroristas del 11 de Septiembre con la aprobación de la Ley Patriota (USA Patriot Act) del 26 de Octubre de 2001. Esta nueva ley amplía la capacidad de las agencias estatales de seguridad para recopilar información de inteligencia dentro de los Estados Unidos, basándose en razones de lucha contra el terrorismo.

En 2008, se añaden enmiendas a la ley FISA, bajo el Gobierno de George W. Bush, que permiten programas de vigilancia masiva a extranjeros, fuera de los Estados Unidos.

En ese momento, el director general de la NSA, Hayden, sugirió numerosos programas y modalidades de vigilancia sin aprobación explícita de los estatutos que, sin embargo, fueron aprobados.

Uno de estos programas fue el *STELLARWIND*, que implicó la colocación de cables de fibra óptica en los principales centros de Internet. Este programa permitía la extracción de datos de las comunicaciones de los ciudadanos estadounidenses, incluyendo comunicaciones por correo electrónico, conversaciones telefónicas, en definitiva, toda la actividad en Internet.

3. ACTUALIDAD: REVELACIONES DE EDWARD SNOWDEN

a) Breve historia de las filtraciones de Edward Snowden

El 9 de junio de 2013, con 29 años de edad, Edward Snowden se mostró a sí mismo como la fuente de las revelaciones de la NSA publicadas esa semana en *The Guardian* y *The Washington Post*, en una entrevista en video con Glenn Greenwald y Laura Poitras.

Edward Joseph Snowden, es un especialista de Tecnologías de la Información, antiguo empleado de la Agencia Central de Inteligencia *(CIA*) y en ese momento trabajador de la Agencia Nacional de Seguridad (*NSA*) a través del contratista americano Booz Allen Hamilton.

Días antes de las revelaciones había abandonado su casa de Hawaii para reunirse en Hong Kong con Poitras, Greenwald y otro periodista del *The Guardian*, Ewen Macaskil.

Snowden quería abrir un debate global sobre los límites de la vigilancia de la NSA. Snowden dijo *"entiendo que sufriré por mis acciones, pero me daré por satisfecho con haber revelado, aunque sólo sea por un instante, el secretismo de las leyes y los irresistibles poderes ejecutivos que gobiernan el mundo hoy en día".*

Snowden ya había dejado los EE.UU. para ir a Hong Kong por temor a represalias legales como resultado de sus filtraciones. Durante varios días permaneció en lugar no revelado en Hong Kong. Sin embargo, pocos días después, los EE.UU. emitieron una orden internacional de arresto contra él por cargos de espionaje. La web de denuncia, *WikiLeaks*, informó que Snowden había embarcado en un vuelo con destino a Rusia, como parada a un país no revelado en Sudamérica.

Se esperaba que Snowden embarcara en un avión con destino a Cuba la mañana siguiente, pero no lo hizo. Su autorización de viaje temporal, expedida por un diplomático ecuatoriano, había sido revocada. Después de pasar varias semanas atrapado en la zona de embarque del aeropuerto Sheremetyevo de Moscú, se le concedió el asilo por un año en Rusia.

Actualmente se encuentran alojado en un lugar no revelado en el país. En octubre de 2013 reapareció en Moscú para ser galardonado con el premio Sam Adams, por la defensa de la integridad y las buenas prácticas de los servicios de inteligencia.

b) ¿Por qué se realizan las revelaciones de Snowden en este momento?

Los documentos revelados por Snowden muestran que la comunidad de la inteligencia de los EE.UU y sus aliados, están involucrados en la vigilancia masiva sin orden judicial de ciudadanos del propio país y extranjeros. Numerosos documentos muestran que, más allá del espionaje realizado con fines de lucha contra el terrorismo, la NSA y sus socios llevaron a cabo el espionaje político e industrial.

A pesar de que son muchos millones de personas a los que le afectan estos sistemas de vigilancia, éstos se han construido sin el conocimiento, autorización o escrutinio de órganos legislativos electos de los EE.UU. y de sus países socios, y mucho menos del público en general. Snowden consideró que esta importante información debería democratizarse, tal y como dijo en unas declaraciones en Junio de 2013:

"Yo sólo soy un tipo que se sienta allí día tras día en la oficina, mira lo que está pasando y se va. Es algo que no está en nuestras manos decidirlo, el público en general necesita decidir si esos programas y políticas son correctas o equivocadas."

c) Conocimiento de otros países sobre los programas de vigilancia de Internet

Las revelaciones de Snowden mostradas a la opinión pública por los medios de comunicación ha arrojado luz sobre las implicaciones de varios tratados secretos firmados por miembros de la UKUSA (tratados Reino Unido – Estados Unidos, de los que son miembros, aparte de los anteriormente citados, los países de Australia, Canadá y Nueva Zelanda), en sus esfuerzos para implementar la vigilancia global.

Según las informaciones sacadas a la luz por Snowden, los países implicados en la vigilancia en masa mundial se dividen en las siguientes categorías:

Cinco ojos (Five-Eyes): A este grupo pertenecen los países implicados en varios tratados secretos firmados por miembros de la UKUSA (tratados Reino Unido – Estados Unidos) en sus esfuerzos para implementar la vigilancia global. A este grupo pertenecen Estados Unidos, Reino Unido, Canadá, Nueva Zelanda y Australia.

Nueve ojos (Nine-Eyes): A este grupo pertenecen los del grupo Cinco Ojos más Dinamarca, Noruega, Países Bajos y Francia.

Catorce ojos (Fourteen-Eyes): Pertenecen los dos grupos anteriores más Alemania, Suecia, Bélgica, España e Italia.

A continuación, veremos cómo se han relacionado estos países y sus diferentes agencias de seguridad e inteligencia con la Agencia Nacional de Seguridad estadounidense (NSA).

Reino Unido

Los servicios de inteligencia francés, alemán, sueco y español tienen desarrollados métodos de vigilancia en Internet y de tráfico telefónico desde 2008, en estrecha colaboración con la GCHQ (agencia de espionaje británica).

El seguimiento en grandes cantidades de datos se realiza a través de intervenciones directas en los cables de fibra óptica, y el desarrollo de las relaciones secretas con las empresas de telecomunicaciones. Una

floja pero creciente alianza de espionaje que ha permitido a las agencias de inteligencia de cada uno de estos países cultivar relaciones con empresas de otros países para facilitar la búsqueda de la web, de acuerdo con los documentos filtrados por Edward Snowden sobre el GCHQ.

En los archivos filtrados también se deja claro que el GCHQ desempeñó un papel principal en el asesoramiento a sus homólogos europeos para trabajar en torno a las leyes nacionales destinadas a restringir el poder de vigilancia de las agencias de inteligencia.

Snowden reveló la existencia del programa *TEMPORA* en el GCHQ, con el que la agencia de inteligencia electrónica se conectaba dentro de los cables de fibra óptica transatlánticos, para llevar a cabo la vigilancia en masa.

La GCHQ dijo en 2008, cuando *Tempora* estaba siendo probado, que el servicio de inteligencia alemán (BND) tenía un enorme potencial tecnológico y un buen acceso al corazón de Internet, que estaban trabajando con algunos portadores (cables de fibra óptica) que funcionaban a 40 Gbps y 100 Gbps. Cuatro años después de este informe, el GCHQ todavía sólo era capaz de controlar cables de 10 Gbps, pero esperaba explotar nuevos portadores de 100 Gbps con el tiempo.

Australia

Otros documentos filtrados por Snowden revelaron detalles de espionaje electrónico del Gobierno de Australia en la región de Asia y Pacífico, mediante una serie de puestos de escucha destinados en misiones diplomáticas.

Se desató una disputa diplomática en la región a raíz de un artículo publicado por *Fairfax media*, que informó acerca de un mapa de alto secreto que detalla 90 instalaciones de vigilancia de los Estados Unidos en las misiones diplomáticas en todo el mundo – incluyendo Camboya, China, Indonesia, Malasia, Myanmar y Tailandia.

Las filtraciones de Snowden muestran los detalles de una operación de inteligencia de Australia para controlar el teléfono móvil del presidente de Indonesia, Susilo Bambang Yudhoyono, de más de 15 días en agosto de 2009.

Como se ha mencionado anteriormente, Australia es parte del acuerdo de inteligencia de UKUSA, también conocido como Cinco Ojos. Su existencia era supuestamente tan secreta que los primeros ministros no tuvieron conocimiento del acuerdo hasta el año 1973, cuando la Commonwealth se llevó a ASIO (servicios de inteligencia australianos), en una reorganización de los organismos de seguridad.

La NSA, por su parte, recibe inteligencia de cuatro instalaciones principales en Australia, que son parte del programa *XKEYSCORE*.

Canadá

Un documento de alto secreto filtrado por Snowden reveló que Canadá había establecido puesto de espionaje para operaciones encubiertas en todo el mundo, llevando a cabo espionaje contra socios comerciales, a petición de la NSA.

Dicho documento filtrado revela que Canadá está involucrada en el enorme organismo de inteligencia de Estados Unidos y en las actividades clandestinas de vigilancia dentro de, aproximadamente, 20 países de alta prioridad.

Las notas informativas dejaron claro que la agencia de inteligencia de Canadá (CSEC) juega un papel importante en la recogida de información en todo el mundo, de manera que se ha ganado el respeto de sus homólogos estadounidenses.

La relación de inteligencia electrónica entre Canadá y Estados Unidos se remonta a más de 60 años. Snowden también informó que las dos agencias cooperaron para permitir que la NSA pudiera espiar a los líderes internacionales en la cumbre del G20 en Toronto, en 2010.

Otro punto en el que se ve esta relación es que la NSA también suministra gran parte del hardware y software que la CSEC utiliza para el cifrado, la decodificación y otros elementos esenciales de espionaje electrónico necesarios para la recogida, el tratamiento y el análisis.

A cambio, la NSA reconoce que su homólogo canadiense ofrece a esta sociedad sus propios productos criptográficos, criptoanálisis, tecnología y software.

Dinamarca

Las revelaciones de Snowden han puesto de manifiesto que Dinamarca tiene una relación de trabajo con la NSA más estrecha que otros muchos países europeos, entre ellos sus vecinos Suecia y Alemania. Este hecho no es de extrañar, ya que según declaraciones de la agencia de seguridad (PET), la inteligencia de este país ha estado estrechamente conectada con la CIA y con otras agencias desde la Segunda Guerra Mundial.

Francia

La primera nota filtrada por Edward Snowden, data del 6 de Agosto de 2007, proviene de la dirección de la NSA. Está sellada como “top secret” (la clasificación más alta), e indica que la relación con la DGSE (dirección general de seguridad externa francesa) está entrando en una nueva dimensión. También se habla de que la discusión entre la dirección de la NSA y la dirección de la DGSE se inició en noviembre de 2006, sobre la necesidad de información y la idea de la creación de un modelo de referencia en términos de colaboración, intercambios no sólo de datos técnicos, sino también en la información que posee cada servicio. En esa nota se felicita a la DGSE por aportar toda su información en esta discusión con la NSA, en África y en las cuestiones contra el terrorismo, como Hezbolá en el Líbano y de AQMI en el Sahel. En estos mismos documentos se refleja que la DGSE ha reforzado su cooperación con el GCHQ británico.

El nivel de cooperación es tal hoy en día que los datos personales procedentes de África o el Oriente Medio, pasando por Francia, y que pertenecen a personas físicas de nacionalidad francesa – hombres de negocio, diplomáticos o agentes de la DGSE en misión – o incluso a los jefes de Estado africanos, pueden caer en las manos de la NSA en el nombre de la lucha contra el terrorismo.

Noruega

La NSA registró más de 33 millones de llamadas telefónicas hechas por Noruega durante un solo mes, en 2012.

Países Bajos

Las dos principales agencias de inteligencia holandesas, la externa MIVD y el servicio de seguridad interno, AIVD, mantienen fuertes relaciones con el GCHQ británico. Según el GCHQ estos organismos son pequeños pero técnicamente competentes y altamente motivados. Les estuvieron proporcionando asesoramiento jurídico, ya que tienen que abordar algunas cuestiones legislativas que les permita operar como otras agencias de inteligencia europeas. Por otro lado, se tiene constancia que la AIVD atacó foros web para recopilar información sobre sus usuarios utilizando una tecnología llamada CNE (*Computer Network Exploitation*).

España

En el caso de la agencia de inteligencia española, el Centro Nacional de Inteligencia (CNI), la clave para la vigilancia de Internet en masa, por lo menos en el 2008, fueron los lazos de los españoles con una empresa de telecomunicaciones británica (no se ha revelado el nombre, ya que las relaciones empresariales están entre los secretos más estrictamente vigilados en la comunidad de inteligencia).

Los informes declaraban también que la agencia de inteligencia británica GCHQ aún no se ha comprometido con el CNI formalmente en la explotación IP, pero el CNI ha estado haciendo grandes avances a través de su relación con un socio comercial del Reino Unido. GCHQ y el socio comercial han sido capaces de coordinar su enfoque. El socio comercial ha proporcionado al CNI algunos equipos, mientras que mantiene informado al GCHQ. Por tanto, se llega a la conclusión de que el GCHQ ha encontrado un homólogo muy capacitado en el CNI, en particular en el ámbito de las operaciones encubiertas de Internet.

Documentos revelados por Snowden muestran que España colaboraba con los servicios secretos estadounidenses, para tener información de inteligencia incluyendo metadatos.

El documento secreto y oficial de la NSA titulado *Sharing computer network operations cryptology information with foreign partners* (Compartiendo información de computación y criptología operacional con socios extranjeros) clasifica la cooperación de los países en cuatro grupos. España está en el segundo grupo denominado de “cooperación centrada”. Los países englobados en este grupo (en total 19, todos

ellos europeos, salvo Japón y Corea del Sur), colaboran en tareas de computación en red, permitiendo recopilar la información a los estadounidenses.

Suecia

La televisión sueca (*Sveriges Television*) revelaba que la agencia de inteligencia sueca (FRA) proporcionó a la NSA datos de su colección por cable, en virtud de un tratado secreto firmado en 1954 para la cooperación internacional en materia de vigilancia.

Por otro lado, Suecia, aprobó una ley en 2008 que permite a su agencia de inteligencia supervisar comunicaciones por correo electrónico y teléfono transfronterizos sin una orden judicial.

Alemania

Se aprecia también conocimiento de dichos programas de espionaje en el Gobierno alemán. El periódico alemán *Der Spiegel* reveló como la agencia de inteligencia del Gobierno alemán (BND) transfiere a la NSA cantidades masivas de datos interceptados.

También otras agencias de seguridad e inteligencia se vieron involucradas en la práctica de vigilancia global.

Israel

La NSA comparte información en bruto con Israel, incluidos los datos de ciudadanos americanos. El acuerdo secreto fue alcanzado a principios de Marzo de 2009, como muestra un documento secreto proporcionado por Snowden a *The Guardian*. Dicho documento demuestra que el Gobierno de EEUU entregó comunicaciones interceptadas que probablemente contenían llamadas telefónicas y correos electrónicos de ciudadanos estadounidenses. El acuerdo no establecía límites legales vinculantes respecto al uso de datos por parte de los israelíes.

Según el acuerdo, la inteligencia que se comparte no se filtra por anticipado por los analistas de la NSA para eliminar las comunicaciones de los Estados Unidos. La NSA envía rutinariamente a la ISNU (Unidad Nacional de señales de inteligencia israelí), una recolección de datos sin tratar.

Aunque el memorándum es explícito al decir que el material tenía que ser manejado de acuerdo con la ley de EEUU, y que los israelíes acordaron no atacar a los americanos identificados en los datos, estas reglas no están respaldadas por obligaciones legales.

En declaraciones a *The Guardian*, un portavoz de la NSA no negó que los datos personales de los estadounidenses se incluyeran en la colección de datos de inteligencia sin tratar compartidos con los israelíes. Pero desde la agencia se insistió que la información compartida cumplió todas las reglas que rigen la privacidad.

d) Colaboración de grandes empresas con las agencias de seguridad e inteligencia

La medida en que las empresas privadas están cooperando con las agencias de inteligencia ha sido una importante fuente de preocupación para los usuarios de Internet en todo el mundo.

Las empresas de tecnología que se mostraban en las diapositivas filtradas por Snowden correspondientes a *PRISM* (programa de vigilancia), tenían muchas ganas de subrayar que no van más allá de lo que se ven obligadas a hacer, en virtud del derecho en la entrega de los datos del usuario, pero otros documentos sugieren que algunas empresas de Internet y de telecomunicaciones, en ocasiones, van más allá de lo que es obligatorio.

Estas relaciones crean problemas de confianza de los clientes para los gigantes tecnológicos de Estados Unidos y del Reino Unido, tal y como reconoció públicamente el fundador de Facebook, Mark Zuckerberg, también planteando preguntas acerca de "*si lo que la ley permite representa los límites de vigilancia, o simplemente un punto de partida*".

Una sentencia judicial de 2011, que fue desclasificada por la Administración del presidente Barak Obama, declaraba inconstitucionales algunas de las actividades de la NSA, porque su incapacidad para separar las comunicaciones electrónicas de los ciudadanos estadounidenses y las de los otros países viola la cuarta enmienda (inviolabilidad de las comunicaciones) de la Constitución.

Un documento secreto de la NSA fechado en diciembre de 2012 y difundido por *The Guardian* refleja los perjuicios que este fallo causó a la agencia, con "un coste de millones de dólares para los proveedores de PRISM", es decir, para las grandes empresas tecnológicas. Los documentos sugieren algunos pagos de PRISM a proveedores de criptografía e interceptación de cable, para acceder a los datos que intercambian los usuarios, pero el alcance de estas operaciones y los receptores son, hasta la fecha, desconocidos. El desembolso en favor de las compañías tecnológicas se produjo después de esta sentencia del Tribunal de Vigilancia de Inteligencia Exterior (FISA).

Las reacciones de las compañías afectadas han sido variadas. Microsoft ha declinado responder a las informaciones del diario, mientras que Google desmiente su cooperación con el programa PRISM y señala que espera que el Gobierno dé respuesta a su petición para poder publicar más datos sobre seguridad nacional. Facebook niega haber recibido cualquier compensación económica. Un portavoz de Yahoo subrayó a *The Guardian* que la ley federal exige al Gobierno el pago de los costes tras el fallo del FISA.

Actualmente las grandes empresas se están uniendo para poner en marcha una reforma de la vigilancia del Gobierno americano. La coalición incluye a Apple, Google, Microsoft, Facebook, Twitter y Yahoo, además de LinkedIn y AOL. Las revelaciones realizadas por Snowden han hecho daño a la imagen que estas empresas tienen fuera de Estados Unidos, lo que puede suponer una pérdida de beneficios, por lo que, ahora, la relación con la NSA les puede perjudicar.

e) Timeline de las revelaciones de Snowden

2013

5 junio → Se anuncia revelaciones de documentos clasificados de la NSA. [*The Guardian*]

6 junio → El programa PRISM se expone públicamente a los estadounidenses. [*The Guardian*]

9 junio → Se revela la identidad de la persona que ha filtrado la información: Edward Snowden. [*The Guardian*]

21 junio → Tempora interviene los cables de fibra óptica. [*The Guardian*]

30 junio → NSA vigila las comunicaciones de los alemanes [*Der Spiegel*]

4 julio → Francia colabora con la NSA [*Le Monde*]

6 julio → Australia ayuda a la NSA en la recolección de datos [*O Globo*]

10 julio → La diapositiva de la NSA explica Upstream, el programa de recolección de datos de PRISM. [*The Washington Post*]

16 julio → Snowden defiende sus actos y explica las razones que le han llevado a realizar las revelaciones. [*The Guardian*]

20 julio → La inteligencia alemana utiliza los programas espías de la NSA. [*Der Spiegel*]

2013

2 Agosto → Las empresas de Telecomunicaciones comparten información de usuarios con la GCHQ. [*The Guardian*]

29 Agosto → La NSA paga millones a las empresas de Telecomunicaciones para tener acceso a los datos. [*The Washington Post*]

9 Septiembre → La NSA puede espiar los datos de los Smartphone. [*Der Spiegel*]

11 Septiembre → La NSA comparte datos 'raw' de inteligencia con Israel. [*The Guardian*]

16 Septiembre → La NSA monitoriza redes financieras. [*Der Spiegel*]

30 Septiembre → Revelado el almacenamiento masivo de metadatos realizado por la NSA. [*Der Spiegel*]

21 Octubre → Estados Unidos monitoriza ciudadanos franceses, empresas y diplomáticos. [*Le Monde*]

22 Octubre → Estados Unidos espía a ciudadanos españoles. [*El Mundo*]

17 Noviembre → Australia espía al presidente de Indonesia. [*The Guardian*]

19 Noviembre → Estados Unidos espía a ciudadanos noruegos. [*Dagbladet*]

28 Noviembre → NSA espió la cumbre del G20 en Toronto. [*Canadian Broadcasting Corporation*]

30 Noviembre → La agencia de inteligencia holandesa espía a usuarios de foros. [*NRC*]

9 Diciembre → NSA y Canadá cooperan. [*Canadian Broadcasting Corporation*]

11 Diciembre → Servicios secretos de Suecia tienen acceso a programas de vigilancia. [*Sveriges Television*]

4. PROGRAMAS DE VIGILANCIA

A continuación realizaremos un análisis de los programas de vigilancia de Internet filtrados por Snowden:

a) PRISM

PRISM es una herramienta utilizada por la Agencia de Seguridad Nacional (NSA), para recoger datos electrónicos privados pertenecientes a los usuarios de los principales servicios de Internet como Gmail, Outlook o Facebook. Es la última evolución de los esfuerzos de vigilancia electrónica a partir del 11 de Septiembre, que comenzaron bajo la presidencia de Bush con la Ley Patriota, y ampliada para incluir la Ley de Vigilancia de Inteligencia Extranjera (FISA), promulgada en 2006 y 2007.

Hay muchas cosas que se desconocen sobre el funcionamiento de PRISM, pero la idea básica es que permite a la NSA solicitar datos de personas concretas a las principales empresas de tecnología como Google, Yahoo, Facebook y Apple. El Gobierno de los EE. UU insiste que sólo se permite recopilar datos cuando se les da el permiso desde el Tribunal de Vigilancia de Inteligencia Extranjera (Tribunal FISA).

Como publicó el periódico *The Washington Post*, la ley para Proteger América de 2007, llevó a la creación de un programa secreto de la NSA denominado US-984XN, también conocido como PRISM. Se dice que el programa es una versión más eficiente de las mismas prácticas que los Estados Unidos estaban llevando a cabo en los años siguientes al 11 de Septiembre, bajo la presidencia de George W. Bush en su Programa de Vigilancia de Terrorismo.

La Ley para Proteger América permite al Fiscal General y al Director Nacional de Inteligencia explicar en un documento clasificado cómo los EE.UU recopilarán datos de inteligencia sobre los extranjeros cada año, pero no especifica los objetivos o lugares concretos. Como informa *The Washington Post*, una vez que el plan se aprueba por un Juez federal en una orden secreta, la NSA puede exigir a empresas como Google o Facebook que envíe datos al Gobierno, siempre y cuando las solicitudes cumplan los criterios del plan clasificado.

¿Qué datos recopila la NSA?

Los programas de la NSA recopilan dos tipos de datos: metadatos y contenido. Los metadatos son el subproducto de las comunicaciones sensibles, como los registros telefónicos que revelan a los participantes, tiempo y duración de las llamadas, las comunicaciones recogidas por PRISM incluyen contenidos de correos electrónicos, chat, llamadas de VoIP y archivos almacenados en la nube.

Las autoridades estadounidenses han tratado de disipar los temores acerca de la recopilación de metadatos de manera indiscriminada por la NSA al señalar que no revelan el contenido de las conversaciones. Pero los metadatos pueden ser tan reveladores como su contenido, por ejemplo, los

metadatos de Internet incluyen información como logs de correo electrónico, datos de geolocalización direcciones IP e historiales de búsquedas en la web. Debido a que la ley tiene décadas de antigüedad, en los EE.UU los metadatos están menos protegidos que el contenido.

Una orden judicial filtrada por Snowden mostró que *Verizon* (compañía de comunicaciones estadounidense), estaba entregando registros de llamadas y metadatos de telefonía de todos sus clientes a la NSA "de forma continua, todos los días."

¿Cómo recopila datos la NSA?

Muchos detalles cruciales sobre cómo y en qué circunstancias recopila datos la NSA son un misterio. En términos legales, los programas de vigilancia se basan en dos leyes fundamentales, la Sección 702 de la Ley de Enmiendas de la FISA (FAA) y la Sección 215 de la Ley Patriota. La primera, autoriza la recopilación de contenido de comunicaciones bajo PRISM y otros programas similares, mientras que la segunda autoriza la recopilación de metadatos de las compañías telefónicas (como el caso de Verizon). Sin embargo, varios informes y documentos filtrados indican que los estatutos han sido interpretados en secreto por los tribunales de inteligencia de la FISA, para garantizar una autoridad mucho más amplia de lo que se permitía originalmente. También se indica que los tribunales de la FISA solamente aprueban los procedimientos de recopilación de datos a la NSA, y no se requieren garantías individuales para los objetivos específicos.

Un analista comienza introduciendo "selectores" (términos de búsqueda), en un sistema como PRISM, los cuales analizan la información desde otros sitios de recopilación, conocidos como SIGADs (Designadores de Actividad de Señales de Inteligencia). SIGADs tiene nombres clave, clasificados y no clasificados, y se encarga de diferentes tipos de datos, como por ejemplo, NUCLEON, que recoge el contenido de conversaciones telefónicas, o MARINA, que almacena metadatos de Internet.

Los documentos filtrados muestran que los analistas de la NSA no pueden localizar específicamente a alguien que razonablemente cree que es una persona de EE.UU, comunicándose en territorio de los EE.UU. Según *The Washington Post*, un analista debe tener al menos un 51 por ciento de certeza que el objetivo es extranjero, pero en el proceso, los datos de comunicación de algunos ciudadanos no extranjeros también se recogen accidentalmente.

El reglamento establece que el analista debe tomar medidas para eliminar los datos de "personas estadounidenses", pero incluso si no son relevantes para el terrorismo o para la seguridad nacional, esas comunicaciones "inadvertidamente recogidas", se pueden conservan y analizar durante un máximo de cinco años, e incluso proporcionárselas al FBI o la CIA, bajo un amplio conjunto de circunstancias. Si las comunicaciones están encriptadas, se pueden mantener indefinidamente.

b) TEMPORA

La agencia de inteligencia GCHQ del Reino Unido, desde el 2008 ha puesto en funcionamiento una red de interceptación masiva llamada *Tempora*, basada en intervenir los cables de fibra óptica, y usada para crear un gran "buffer de Internet", con enormes cantidades de datos que fluyen desde dentro y fuera del Reino Unido.

El contenido de las comunicaciones recogidas por el sistema se almacena durante tres días, mientras que los metadatos (remitente, destinatario, tiempo) son almacenados durante treinta.

El sistema es activado usando una cláusula poco conocida de una ley aprobada en el año 2000 para la vigilancia individual garantizada, llamada RIPA. Las compañías de telecomunicaciones que se vieron involucradas en el programa según los documentos filtrados por Snowden fueron BT, Verizon Business, Vodafone Cable, Global Crossing, Level 3, Viatel e Interoute.

Los documentos revelan que durante el último año la GCHQ había manejado 600 millones de eventos telefónicos cada día, había intervenido más de 200 cables de fibra óptica y que era capaz de procesar datos de al menos 46 de ellos a la vez.

Cada uno de los cables lleva datos a una velocidad de 10 gigabits por segundo, por lo que los cables interceptados tenían la capacidad, en teoría, de servir más de 21 petabytes al día, equivalente a enviar toda la información de todos los libros de la Biblioteca Británica 192 veces cada 24 horas. Y la escala del programa está constantemente incrementándose con más y más cables interceptados, y las instalaciones de almacenamiento de la GCHQ en Reino Unido y en el extranjero se expanden con el objetivo de procesamiento de datos en terabits a la vez.

Los centros de procesamiento aplican una serie de sofisticados programas de ordenador con el fin de filtrar el material a través de lo que se conoce como MVR (reducción masiva del volumen). El primer filtro rechaza inmediatamente el alto volumen, el tráfico de escaso valor, como las descargas peer-to-peer, lo que reduce el volumen un 30 por ciento. Otros retiran los paquetes de información relativa a los "selectores" (búsqueda de términos incluyendo temas, números de teléfono y correos electrónicos de interés). La mayor parte de la información extraída es contenido, como grabaciones de las llamadas telefónicas o el cuerpo de los mensajes de correo electrónico. El resto son metadatos.

La legitimidad del uso del programa está en duda. De acuerdo con los dictámenes jurídicos del GCHQ, se le dio el visto bueno mediante la aplicación de la ley antigua a la nueva tecnología. La Ley 2000 de Regulación de Poderes de investigación (RIPA), necesita que la intervención defina los objetivos para ser autorizados por una orden firmada por el Ministro del Interior o el Secretario de Relaciones Exteriores. Sin embargo, una cláusula permite que el Secretario de Relaciones Exteriores pueda firmar un certificado para la interceptación de amplias categorías del material, siempre y cuando uno de los extremos de las comunicaciones monitorizadas es extranjero. Sin embargo, la naturaleza de las comunicaciones de fibra

óptica modernas hace que una proporción del tráfico interno del Reino Unido se retransmita al extranjero para volver a continuación por los cables.

El Parlamento aprobó la ley RIPA para permitir que GCHQ recupere la información.

c) UPSTREAM

Es un término utilizado por la NSA para denominar la interceptación del tráfico telefónico y de Internet de los principales cables y conmutadores, tanto nacionales como extranjeros.

Según una de las diapositivas filtradas por Snowden, se describe *Upstream* como una *"recopilación de las comunicaciones en los cables de fibra e infraestructuras de datos"*. Dicha recopilación se lleva a cabo bajo los siguientes programas de vigilancia:

- FAIRVIEW
- STORMBREW
- BLARNEY
- OAKSTAR

Los programas FAIRVIEW, STORMBREW y BLARNEY recopilan datos en instalaciones de los Estados Unidos, mientras que OAKSTAR es un paraguas para ocho programas diferentes usados para recopilar datos fuera de este país. Bajo estos cuatro programas, la recopilación se lleva a cabo en cooperación con empresas de telecomunicaciones, nacionales y extranjeras.

Upstream permite el acceso a grandes volúmenes de datos. Una primera preselección se hace en el proveedor de telecomunicaciones, el cual selecciona el tráfico de Internet que muy probablemente contiene comunicaciones extranjeras. Luego los datos se pasan a la NSA, donde se realiza una segunda selección, copiando el tráfico y filtrándolo, usando lo que se denomina "selectores fuertes" como son números de teléfono, correos electrónicos o direcciones IP de personas y organizaciones en las que esté interesada la NSA.

Según esta información, hay más de una docena de estaciones de conmutación en los EE.UU, en los que se instalan este tipo de filtros. Para recopilar datos de cables de fibra y conmutadores fuera de allí, la NSA ha tenido acuerdos con proveedores de Internet extranjeros, especialmente en Europa y Oriente Medio.

Revelaciones posteriores informaron que la NSA mantiene todos los metadatos que obtiene a través de Upstream y PRISM en un sistema de base de datos llamado MARINA durante 12 meses.

d) XKEYSCORE

Es un sistema de explotación DNI y un framework analítico. DNI se refiere a la inteligencia de la red digital, es decir, la inteligencia derivada del tráfico de Internet. Los inicios de este sistema se remontan al año 2008.

XKeyscore se compone de más de 700 servidores en aproximadamente 150 sitios en los que la NSA recoge los datos, como son EE.UU., aliados militares y cuatro bases en Australia y una en Nueva Zelanda, así como embajadas y consulados de Estados Unidos en muchos países de todo el mundo.

De acuerdo con los documentos filtrados por Snowden, esos servidores se alimentan con datos que provienen de los siguientes sistemas de recopilación:

- F6: Servicio Especial de Recopilación. Operación conjunta de la CIA y la NSA que llevan a cabo operaciones clandestinas, incluyendo el espionaje de diplomáticos y líderes extranjeros.
- FORNSAT: Significa recopilación de satélites extranjeros, y se refiere a interceptar satélites.
- SSO: Fuente de Operaciones Especiales. Una división de la NSA que colabora con los proveedores de telecomunicaciones.

A partir de estas fuentes, XKeyscore almacena todos los datos que recupera, los cuales son indexados mediante plugins que extraen cierto tipo de metadatos (como números de teléfono, direcciones de correo electrónico, logs y actividades de usuario) y los indexan con tablas de metadatos, las cuales se consultan por analistas. XKeyscore se ha integrado con MARINA, la base de datos de metadatos de Internet de la NSA.

A los analistas, Xkeyscore les permite consultar terabytes de información en bruto recogidos desde los sitios de recopilación anteriormente mencionados. De esta manera, encuentran objetivos que no podrían localizar buscando sólo por los metadatos, y también pueden hacer esto contra un conjunto de datos que de otra manera podrían haber sido desechados por sistemas de procesamiento front-end.

Debido a que XKeyscore mantiene el tráfico de las comunicaciones en bruto, los analistas no sólo pueden realizar consultas utilizando selectores “fuertes”, como direcciones de correo, sino que también pueden utilizar selectores “blandos”, como palabras clave en los textos del cuerpo del correo electrónico, mensajes de chat o documentos digitales en varios idiomas.

XKeyscore también tiene las siguientes capacidades:

- Búsqueda del uso de Google Maps y sus términos introducidos en el motor de búsqueda de objetivos conocidos para localizar cosas o lugares sospechosos.
- Búsqueda de anomalías y sin ninguna persona específica adjunta, como la detección de la nacionalidad de los extranjeros mediante el análisis del lenguaje utilizado en correos electrónicos interceptados.
- Detectar las personas que usan cifrado.
- Mostrar el uso de redes privadas virtuales (VPNs) y máquinas que pueden ser potencialmente atacadas.
- Seguimiento de la fuente y autoría de un documento que ha pasado a través de muchas manos.

e) BULLRUN

La NSA ha estado realizando esfuerzos sistemáticos para debilitar el cifrado, la tecnología que sostiene la protección y la seguridad de Internet, incluyendo cuentas de correo electrónico, comercio, banca y registros oficiales.

Desde el 2010, La NSA tiene un programa de 250 millones de dólares al año para trabajar de manera abierta y encubierta con la industria criptográfica, para debilitar el software de seguridad, el equipo de hardware y las normas globales en seguridad. El proyecto incluía la creación de puertas traseras en los sistemas de seguridad y el uso y explotación de las vulnerabilidades detectadas en el software.

El programa utilizado por la NSA para estos propósitos es *Bullrun*. Las revelaciones de Snowden no ofrecen demasiados detalles del funcionamiento de este programa, ya que no tenía acceso a esta información, pero por la documentación filtrada podemos ver que el acceso al programa se limitaba a un grupo reducido de personal con alto rango de las agencias de inteligencia pertenecientes al grupo de los "Cinco Ojos".

Los datos que no se pueden descifrar pueden ser retenidos indefinidamente mientras las agencias continúan intentando descifrarlos.

Bullrun tiene capacidad para romper el cifrado de protocolos como TLS/SSL, HTTPS, SSH y VoIP; redes como VPN, clientes de correo como *Webmail*, incluyendo otras tecnologías de comunicación por red que no están detalladas en las filtraciones.

Por otro lado, la agencia británica GCHQ tiene un programa de similares características llamado *Edgehill*.

f) Tabla Resumen Programas de vigilancia

La siguiente tabla nos da una visión general y resumida de los programas de vigilancia en Internet:

NOMBRE	PAIS ORIGEN	CREACIÓN	CONOCIMIENTO de su EXISTENCIA	ACCESO DATOS	ALMACENA INFORMACION	ALCANCE
ECHELON	EEUU	1977	1999	TIEMPO REAL	SI	GLOBAL
STELLARWIND	EEUU	2001	2009	ALMACENADOS	SI	GLOBAL
TEMPORA	REINO UNIDO	2008	2013	TIEMPO REAL	SI	GLOBAL
PRISM	EEUU	2007	2013	ALMACENADOS	SI	GLOBAL
UPSTREAM	EEUU	2007	2013	TIEMPO REAL	SI	GLOBAL
XKEYSCORE	EEUU	2008	2013	ALMACENADOS	SI	GLOBAL
BULLRUN	EEUU	2010	2013	TIEMPO REAL/ALMACENADOS	SI	GLOBAL

Figura 5. Programas de vigilancia

5. MEDIDAS DE PROTECCIÓN FRENTE A LOS PROGRAMAS DE VIGILANCIA

Como hemos visto con anterioridad, la manera de recopilar datos por parte de los programas de vigilancia es a través de la red. Así que el principal esfuerzo que tiene que hacer el usuario para mantener su privacidad es proteger sus comunicaciones a través de Internet.

Las medidas recomendadas para evitar que cualquier persona pueda ser espiada al conectarse a la red e intercambiar información son las siguientes:

a) Cifrar las comunicaciones

Para ello hay diferentes técnicas:

1. Usar el cifrado end-to-end

Cifrar el contenido de comunicación en todo el recorrido, de un extremo de la comunicación al otro. Es un sistema de cifrado que transfiere los datos del emisor al receptor de forma segura. El emisor codifica y el receptor descodifica, sin que interfieran terceros. Este tipo de cifrado se utiliza para la capa de aplicación y se tiene en cuenta para los siguientes tipos de comunicaciones:

- ***Servicios de mensajería instantánea***

Las aplicaciones de mensajería instantánea (IM), se han popularizado actualmente gracias a la enorme difusión de los dispositivos móviles. Ejemplo de ello son aplicaciones propietarias pero gratuitas como *WhatsApp* o *Line* que acumulan millones de usuarios en todo el mundo.

Para cifrar conversaciones de mensajería instantánea se puede utilizar *Off-the-Record Messaging* (*OTR*), evitando que el proveedor de mensajería instantánea pueda leer dichas conversaciones. Este protocolo criptográfico sólo funciona con proveedores de mensajería instantánea que permiten el uso de software de mensajería instantánea externa, además, el usuario tendrá que instalar en su dispositivo una aplicación de mensajería instantánea capaz de soportar OTR.

OTR utiliza una combinación del algoritmo de clave simétrica AES, el intercambio de claves Diffie-Hellman y la función hash SHA-1. Se establece un intercambio de claves privadas entre las partes implicadas en la conversación. De esta manera, dichas partes quedan autenticadas y se aseguran que quién les está hablando es ciertamente esa persona y no un impostor. Por otro lado, este cifrado evita que alguien en la red pueda leer los mensajes. Si alguno de los usuarios pierde las claves privadas, ninguna conversación anterior se ve comprometida, ya que los mensajes se cifran con claves AES temporales.

OTR sólo puede proteger las conversaciones cuando todos los usuarios que entablan una conversación tienen un cliente que soporte OTR. Existen versiones de mensajería instantánea a través de un navegador web, como *Cryptocat*, que también utiliza OTR.

A continuación, exponemos un listado de programas de mensajería instantánea que soportan OTR (entre paréntesis los sistemas operativos y las tecnologías en los que están disponibles):

Adium (OS X): Soporta los diferentes sistemas de mensajería instantánea más utilizados, como *Google Talk*, *Windows Live Messenger*, *Yahoo! Messenger* y *Facebook Chat*. Puede transferir archivos. Permite al usuario poder iniciar la sesión en varios servicios desde esta aplicación gracias a una biblioteca llamada *libpurple*, que puede trabajar con los diferentes protocolos de mensajería instantánea.

Cryptocat (GNU/Linux, BSD, OS X, Windows): Sistema de mensajería instantánea dentro de un navegador web.

Pidgin (GNU/Linux, BSD, Windows): Similar a Adium, también trabaja con la biblioteca *libpurple*.

ChatSecure (Android, iOS): Trabaja bajo el protocolo de comunicación para mensajes *XMPP (Extensible Messaging and Presence Protocol).*

- ***Cifrar correos electrónicos***

Entre las técnicas para cifrar y descifrar correos electrónicos destacamos *Pretty Good Privacy* (*PGP*).

PGP es un programa de ordenador de cifrado y descifrado de datos que proporciona privacidad y autenticación criptográfica para la comunicación de datos. PGP se usa no sólo para firmar, codificar y descodificar correos electrónicos, si no también textos, archivos y particiones enteras de disco para incrementar la seguridad de las comunicaciones por correo electrónico. Fue creado por Phil Zimmermann en 1991.

OpenPGP es el protocolo de código abierto que define cómo funciona el protocolo PGP. Existe una versión gratuita del programa llamada GPG, compatible con la versión propietaria.

PGP utiliza diferentes procesos de cifrado, los cuales garantizan la seguridad desde el momento en que cifras un archivo, mensaje o documento y lo descifras. PGP genera su propia clave PGP llamada clave de pares, que se divide en dos partes: clave pública y clave secreta. Con esa clave pública se pueden cifrar los mensajes y verificar firmas que se han generado con la clave secreta. Con esa clave secreta se puede descifrar mensajes cifrados con la clave pública y firmar digitalmente los mensajes. Cada emisor y receptor tiene una clave secreta que sólo es conocida por cada uno de ellos, por lo que mejora la seguridad. Además las claves secretas se cifran con una contraseña, por lo que hacen más difícil a un atacante conseguir el contenido de esta clave.

Por otro lado, en el proceso de cifrado se comprime el mensaje a enviar, haciendo que se ahorre tiempo de transmisión y aumente la dificultad para descifrar el mensaje con técnicas comunes de criptoanálisis.

El problema de PGP es que no es fácil de utilizar, ya que es necesario que el usuario cree, gestione e intercambie claves de manera manual.

2. Uso de VPN

Una VPN (*Virtual prívate network*) crea un túnel encriptado para que pasen datos a través de él, permitiendo que el dispositivo envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada de manera segura, haciendo complicado realizar escuchas.

Las redes VPN trabajan en la capa de red, usando protocolos de seguridad como *IPSec* (IP seguro). En el caso de este protocolo se puede encapsular el tráfico de metadatos, para que sólo se pueda desencapsular cuando se llegue al receptor de la comunicación, haciendo difícil la extracción de información por parte de un atacante.

Otra alternativa de las VPN en la capa de aplicación sería utilizar protocolos criptográficos TLS/SSL para cifrar el tráfico. Se ha probado que son muy seguros y siguen siendo sometidos a constantes mejoras y pruebas.

Cuando se utiliza un servicio VPN, el proveedor de servicios de Internet (*ISP*), no puede descifrar lo que se está transmitiendo, pero sí puede ver que está conectado a sus servidores mediante una IP, aparte de la cantidad de datos transmitida y si se están utilizando datos cifrados. Si no se mantiene ningún tipo de registro en la red virtual creada, la VPN preservará la privacidad y el anonimato.

3. Sospechar del software de cifrado de grandes empresas o propietario

Debido a las revelaciones realizadas por Snowden sobre los programas criptográficos y la relación de la NSA con grandes compañías del sector, hace sospechar que dicho software pueda contener “puertas traseras” por donde sea más fácil acceder a las agencias de seguridad.

Se recomienda utilizar software de cifrado de domino público compatible con otras implementaciones.

b) Uso de protocolos de comunicación seguros

El protocolo que utilizamos para mantener seguras nuestras comunicaciones con los sitios web, mientras nuestros datos viajan por Internet es HTTPS (HTTP seguro).

Los navegadores web soportan HTTPS, pero la conexión con sitios web puede no ser segura. El problema es que sólo se puede mantener una conexión segura con un sitio web si éste sitio ofrece una conexión HTTPS. Por tanto, para evitar que terceras personas puedan obtener nuestros datos cuando nos conectamos a sitios web, confiaremos en los que puedan ofrecernos esa conexión HTTPS.

c) Anonimato y privacidad en la red: Tor

Tor es un programa que permite utilizar Internet mientras oculta su dirección IP, que es, normalmente una representación bastante exacta de la ubicación de la persona que navega por Internet.

Inicialmente Tor fue desarrollado por el Laboratorio de Investigación Naval de los Estados Unidos, con el propósito principal de proteger las comunicaciones gubernamentales.

La red Tor es una red de túneles virtuales que se compone de más de 3600 servidores voluntarios llamados nodos. Cuando alguien utiliza la red Tor para visitar un sitio web, su conexión viaja a través de tres de esos nodos (llamado circuito), antes de salir a la conexión normal de Internet. Cualquiera que intercepte el tráfico de su conexión pensará que su ubicación está en el nodo final de donde todo el tráfico sale. De esta manera, los programas de vigilancia de Internet, que espían en múltiples partes de la red, tendrán más problemas para analizar el tráfico de datos, ya que se distribuyen las transacciones entre distintos lugares de Internet, de esta manera un único punto no puede vincular a los datos con su destino. Los datos, en lugar de tomar una ruta directa desde el origen al destino, toman caminos aleatorios a través de varios repetidores (servidores) que tapan su rastro para que ningún observador en un único punto pueda decir de dónde proceden los datos o adónde se dirigen.

Para crear una ruta de red privada con Tor, el cliente construye de manera incremental un circuito de conexiones cifradas a través de repetidores en la red. El circuito se extiende un tramo cada vez, y cada repetidor, a lo largo del camino, conoce únicamente qué repetidor le proporciona los datos y a qué repetidor se los tiene que entregar. Ningún repetidor individual conoce el recorrido completo de los datos. El cliente negocia por separado un conjunto de claves de cifrado para cada tramo, así se asegura que estas conexiones no se pueden rastrear.

Tor sólo funciona con flujos TCP y puede usarse con cualquier aplicación que soporte SOCKS (Socket Secure).

La gran cantidad de personas que utilizan Tor es lo que le hace tan seguro. Tor esconde a cada individuo entre los otros usuarios de la red, así que cuanto más poblada y diversa sea su base de usuarios, más se protegerá el anonimato de los mismos.

Existe un navegador web, llamado *Tor Browser*, que envía la totalidad de su actividad de navegación a través de la red Tor.

Otras herramientas que también preservan el anonimato en la red (entre paréntesis, los sistemas operativos en los que está disponible):

Orbot (Android)

Freenet (GNU/Linux, BSD, OS X, Windows)

GNUNet (GNU/Linux, BSD, OS X, Windows)

I2P (GNU/Linux, BSD, OS X, Windows)

Syndie (GNU/Linux, OS X, Windows)

El programa Tor se cita explícitamente en las revelaciones proporcionadas por Edward Snowden. Documentos de alto secreto de la NSA, revelan que los éxitos actuales de la agencia contra Tor se basan en identificar a los usuarios y después atacar el software vulnerable de sus equipos. Una técnica desarrollada por la NSA fija como objetivo el navegador web Firefox que se usa con Tor, dando a la agencia el control total de las actividades de los ordenadores objetivos.

Pero esos mismos documentos sugieren que la seguridad fundamental del servicio Tor permanece intacta, ya que muestra la incapacidad por parte de la agencia de sacar del anonimato a todos los usuarios de Tor. Asimismo, la agencia reconoce que no ha tenido ningún éxito para sacar del anonimato a un usuario en respuesta a una petición específica.

A pesar de la importancia de Tor para periodistas, activistas y defensores de los derechos humanos y disidentes para mantener la privacidad de las comunicaciones y evitar las represalias de sus gobiernos, la NSA y la GCHQ creen que también es utilizado por terroristas, pederastas y narcotraficantes, por ello los continuos esfuerzos para poder atacar este sistema.

d) Motores de búsqueda de Internet

La mayoría de los motores de búsqueda de Internet ofrecen una manera rápida de encontrar información, pero también almacenan información del usuario como puede ser su dirección IP, su ubicación física, fecha y hora de la búsqueda, términos de búsqueda, ID cookies (identifica de manera única a un ordenador), e incluso historiales y hábitos de navegación del usuario.

Para mantener el anonimato al realizar búsquedas en Internet, el usuario debería utilizar motores de búsqueda sin seguimiento o anónimos, además de no compartir la información de búsqueda con terceros.

Algunos ejemplos de estos motores de búsqueda son (entre paréntesis la tecnología o sistema operativo para los que se ofrece):

Disconnect Search (Web Services)

DuckDuckGo (Web Services)

Ixquick (Web Services)

MetaGer (Web Services)

Seeks Project (GNU/Linux)

Startpage (Web Services)

YaCy (GNU/Linux, OS X, Windows)

e) Privacidad en las llamadas telefónicas por Internet: Cifrar VoIP

Para evitar que se puedan realizar escuchas a las llamadas telefónicas por Internet de los ciudadanos utilizando la tecnología VoIP (*Voice over IP*), se necesita cifrar esa comunicación. Las tecnologías de cifrado utilizadas en las llamadas de Internet así como el tipo y nivel de protección usado varían enormemente.

Muchas herramientas de telefonía y vídeo por Internet proporcionan algún tipo de cifrado, pero no tienen ninguna protección contra el proveedor del servicio. Es decir, que la empresa que proporciona esa herramienta puede espiar o verse obligada a espiar una conversación sin que el usuario pueda hacer nada por evitarlo.

Existen herramientas de cifrado end-to-end para VoIP. Un protocolo muy útil para realizar el cifrado es *ZRTP* (Z-*Real Time Transport Protocol*). ZRTP es un protocolo criptográfico de acuerdo de claves secretas, para negociar el cifrado entre los dos puntos de conexión de una llamada telefónica sobre VoIP. Está basado en el protocolo de transporte a tiempo real. ZRTP no requiere una infraestructura de clave pública, ya que utiliza el intercambio de claves Diffie – Hellman, que se generan en cada conexión, y el protocolo de transporte a tiempo real seguro (*Secure Real-time Transport Protocol – SRTP*). De este modo, cada una de las partes de la conexión marca a la otra como "parte de confianza".

Al igual que con los programas de mensajería instantánea, sólo se podrá recibir llamadas seguras si la persona que llama utiliza un programa compatible con esta tecnología.

6. *CONCLUSIONES*

Analizando la información filtrada por Snowden y la publicada por los medios de comunicación, observamos que los diferentes gobiernos eran conscientes de esta vigilancia masiva a nivel global y que incluso la aplicaban y participaban en acuerdos de intercambio de información personal entre sus agencias de seguridad e inteligencia y la Agencia Nacional de Seguridad (NSA) de Estados Unidos.

Aunque Israel es uno de los aliados más cercanos de Estados Unidos, no pertenece el grupo conocido como Cinco Ojos (Five-Eyes), que es según las categorías definidas por la NSA, el núcleo principal de los países que participan en el intercambio de vigilancia con los EE.UU.

Algunos gobiernos, como el alemán, francés y español han reaccionado con enfado a los informes basados en la NSA y filtrados por Snowden desde junio de 2013, que revelan la interceptación de las comunicaciones de decenas de millones de sus ciudadanos cada mes. Los funcionarios de inteligencia de Estados Unidos han insistido en que la vigilancia de masas también se lleva a cabo por los organismos de seguridad de los países involucrados, y que son compartidas con los EE.UU. Por eso, la NSA encuadra en otras dos categorías a los países implicados en la vigilancia masiva: Nueve Ojos (Nine-Eyes) y Catorce Ojos (Fourteen-Eyes).

También, los documentos muestran que el Reino Unido, y concretamente su agencia GCHQ, se ha hecho un puente indispensable entre Estados Unidos y los espías de Europa.

Estas revelaciones dan a entender que también existe un conocimiento de esta vigilancia masiva por parte de las grandes empresas tecnológicas, como proveedores de telecomunicaciones, servicios de Internet y software de cifrado, que incluso apoyan, suministran datos y ofrecen cobertura a las agencias de seguridad de los países que están trabajando conjuntamente con la NSA, además de permitir el uso de vulnerabilidades en sus productos.

Por otro lado, se han analizado los sistemas de vigilancia de Internet que han desarrollado la NSA y la GCHQ, como son PRISM, Tempora, Upstream, XkeyScore y Bullrun, desglosando las principales características de alcance de los sistemas, y cómo analizan, almacenan y tratan los datos recopilados.

Por toda esta información hemos destacado unas medidas concretas con sus herramientas para dar solución a los problemas de privacidad que han derivado de esta situación, incluyendo el cifrado de datos o evitar el rastreo de acceso a sistemas o búsquedas en Internet. En este sentido, concluimos que Tor es el método más efectivo para mantener la privacidad, ya que las revelaciones por parte de Snowden muestran la incapacidad de la NSA, hasta la fecha, de sacar del anonimato a un usuario.

A día de hoy, se siguen produciendo de manera periódica revelaciones por parte, principalmente, de los periódicos *The Guardian* y *The Washington Post,* y de medios de comunicación de los países implicados en esta vigilancia masiva, provenientes de las filtraciones producidas por Edward Snowden. Así que es posible que podamos conocer más detalles de los programas de vigilancia de Internet tanto de la NSA como de la GCHQ, y sus relaciones con los países aliados y sus agencias de seguridad.

Dada la enorme difusión en los últimos tiempos de los sistemas móviles, principalmente teléfonos móviles inteligentes, que se cuentan por millones en todo el mundo, se podrían incluir como ampliación del

trabajo o como objeto concreto de estudio, por el interés que suscita para las agencias de espionaje. Como ya informó el periódico *Der Spiegel* en Septiembre de 2013, la NSA podía tener acceso a los datos de cualquier terminal de telefonía móvil, ya que podía romper la seguridad de sus sistemas operativos.

También, otra posible futura ampliación, podría ser el estudio y el análisis de las leyes que controlan la privacidad en Internet, de cada gobierno implicado en esta vigilancia masiva, incluyendo las leyes o las normativas por las que se rigen sus agencias de seguridad para recopilar los datos de los ciudadanos y qué consecuencias tienen en éstos.

7. GLOSARIO

AIVD Agencia de inteligencia interna holandesa.

ASIO Servicios de inteligencia australianos.

BND Agencia de espionaje alemana.

Blarney Véase **Upstream**

Bullrun Programa de la NSA para romper la tecnología de cifrado que protege las cuentas de correo electrónico, transacciones bancarias y registros oficiales. Los servicios de inteligencia del Reino Unido tienen un programa similar, llamado *Edgehill*.

CNI Centro Nacional de Inteligencia de España.

CSEC Agencia de inteligencia de Canadá.

DGSE Dirección General de Seguridad externa francesa.

DNI (digital network information) Datos enviados a través de redes informáticas, como solicitudes a páginas web, correos electrónicos o voz sobre IP.

Edgehill Véase **Bullrun**.

FISA (Tribunal) Tribunal de vigilancia de inteligencia extranjera, un tribunal secreto de los Estados Unidos que supervisa la vigilancia conforme a la ley FISA.

Fairview Véase **Upstream**.

Five Eyes Grupo *Cinco ojos* formado por países angloparlantes que comparten inteligencia. Lo componen Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda.

Fourteen Eyes Grupo Catorce Ojos. A este grupo pertenecen los del grupo **Nine Eyes** más Alemania, Suecia, Bélgica, España e Italia.

FRA Agencia de inteligencia de Suecia.

GCHQ Cuartel general de las Comunicaciones Gubernamentales (*Government Communications Headquarters*). Agencia de inteligencia del Reino Unido centrada en tratar señales y comunicaciones de inteligencia.

ISNU Unidad Nacional de Señales de Inteligencia israelí.

MARINA La base de datos donde la NSA almacena metadatos de millones de usuarios de Internet por un periodo de hasta un año.

Metadatos Datos que identifican una llamada telefónica o un correo electrónico, que podrían incluir el tiempo, la duración, los números de teléfono o direcciones de correo, y la ubicación de ambas partes de la comunicación.

MIVD Agencia de inteligencia externa holandesa.

Nine Eyes Grupo *Nueve Ojos*. A este grupo pertenecen los del grupo **Five Eyes** más Dinamarca, Noruega, Países Bajos y Francia.

NSA Agencia Nacional de Seguridad (National Security Agency) de los Estados Unidos, responsable de la recogida y análisis de información de inteligencia, además de encargarse de la ciberseguridad.

Oakstar Véase **Upstream**.

Patriota (Ley) Ley creada por los Estados Unidos en 2001 para ampliar la capacidad de las agencias de seguridad estatales para recopilar información de inteligencia dentro y fuera del país.

PET Agencia de seguridad de Dinamarca.

Prism Programa de la NSA para recoger datos de grandes empresas de Internet.

SSL (Secure Sockets Layer) Protocolo criptográfico predecesor de TLS. Véase **TLS**.

Stellarwind Programa creado por la NSA que permite la extracción de datos de los cables de fibra óptica de las comunicaciones de los ciudadanos estadounidenses.

Stormbrew Véase **Upstream**.

Tempora Sistema de la GCHQ para crear un buffer de Internet a gran escala, almacenando contenido de Internet durante tres días y metadatos hasta treinta días.

TLS (Transport Layer Security) Protocolo criptográfico que proporciona seguridad cifrando los datos de las conexiones de red en la capa de aplicaciones.

Tor Software libre que permite a los usuarios comunicarse de manera anónima.

UKUSA Tratado de Seguridad creado por el Reino Unido y Estados Unidos, al que se le han ido añadiendo otros países como Canadá, Australia y Nueva Zelanda.

Upstream Término utilizado por la NSA que se refiere a los programas de interceptación masiva, llamados Stormbrew, Oakstar and Blarney, para interceptar enormes cantidades de datos de los cables de comunicación de fibra óptica.

Verizon Uno de los proveedores de telecomunicaciones más grandes de América, del cual la NSA recopilaba registros telefónicos (metadatos) de millones de clientes.

XKeyscore Programa de la NSA que permite a los analistas buscar en enormes bases de datos de correos electrónicos, chats en línea y en los historiales de navegación de millones de personas, sin autorización previa.

8. BIBLIOGRAFIA

Listado de los recursos bibliográficos utilizados, por orden de aparición en el Trabajo de Fin de Máster:

(2013) “The US surveillance programs and their impact on EU citizens' fundamental rights”. *European Parliament* [Fecha de consulta: 2 de Abril de 2014]
<http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf>

Laurie. (2007, 7 de Junio) "A very brief history of US government Internet surveillance programs". [Fecha de consulta: 30 de Marzo de 2014]
<http://seldo.com/weblog/2013/06/07/a_very_brief_history_of_us_government_internet_surveillance_programs>

Morales Luna, G. (2013, 7 de Mayo) "Turing y Bletchley Park". [Fecha de consulta: 30 de Marzo de 2014]
<http://delta.cs.cinvestav.mx/~gmorales/12Enigma/node3.html>

"Bletchley Park, Historia temprana, Segunda Guerra Mundial, Después de la guerra, Bletchley Park Trust, Museum Atracciones, En la cultura popular". *centrodeartigos.com.*[artículo en línea] [Fecha de consulta: 30 de Marzo de 2014]
<http://centrodeartigos.com/articulos-utiles/article_103848.html>

"Alan Turing". *Wikipedia* [artículo en línea] [Fecha de consulta: 30 de Marzo de 2014]
<http://es.wikipedia.org/wiki/Alan_Turing>

Criado, M. A. (2014, 5 de Febrero) " Colossus, el ordenador que ayudó a ganar la II Guerra Mundial, vuelve a la vida”. [Fecha de consulta: 30 de Marzo de 2014]
< http://www.huffingtonpost.es/2014/02/05/colossus-aniversario_n_4728711.html>

Corera , G. (2013, 30 de Octubre) “Escándalo de espionaje: qué es el "Club de los cinco ojos" ". [Fecha de consulta: 30 de Marzo de 2014]
<http://www.bbc.co.uk/mundo/noticias/2013/10/131030_internacional_estados_unidos_espionaje_reino_unido_club_cinco_ojos_az.shtml>

"Código Enigma, descifrado: el papel de Turing en la Segunda Guerra Mundial". *eldiario.es* [artículo en línea] [Fecha de consulta: 30 de Marzo de 2014]
<http://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_0_226078042.html>

"La Red Echelon=La Gran Oreja". [Fecha de consulta: 30 de Marzo de 2014]
<http://www.bibliotecapleyades.net/ciencia/echelon02.htm#Qu%C3%A9%20es%20la%20Red%20Echelon

"ECHELON. ONLINE SURVEILLENCE. ECHELON intercept station at Menwith Hill, England". *CAQ (CovertAction Quarterly).*[Fecha de consulta: 30 de Marzo de 2014]
<http://whatreallyhappened.com/RANCHO/POLITICS/ECHELON/echelon.html>

Campbell, D. "Inside Echelon. The history, structure and function of the global surveillance system known as Echelon". [Fecha de consulta: 30 de Marzo de 2014]
<http://www.bibliotecapleyades.net/ciencia/echelon01.htm>

"ECHELON UKUSA Alliance"(2007). *world-information.org* [artículo en línea] [Fecha de consulta: 30 de Marzo de 2014]
<http://world-information.org/wio/infostructure/100437611746/100438658806?opmode=contents>

Maldonado, C. E.(2013, 9 de julio) "La red Echelon: el control de internet y de todas las comunicaciones". [Fecha de consulta: 31 de Marzo de 2014]
< http://www.eldiplo.info/portal/index.php/extensions/k2/on-the-scene/item/415-la-red-echelon-el-control-de-internet-y-de-todas-las-comunicaciones>

(2001, 10 de septiembre) "Echelon: la tecnología avanzada al servicio del autoritarismo". [Fecha de consulta: 31 de Marzo de 2014]
<http://www.lr21.com.uy/mundo/55528-echelon-la-tecnologia-avanzada-al-servicio-del-autoritarismo>

(2013) *The Guardian* - The NSA files [Fecha de consulta: 2 de Abril de 2014]
< http://www.theguardian.com/world/the-nsa-files>

González, J. C. (2001, 8 de Marzo) " Una comisión de la Eurocámara confirma la existencia de Echelon". *El Mundo* [artículo en línea] [Fecha de consulta: 31 de Marzo de 2014]
< http://www.elmundo.es/navegante/2001/03/08/seguridad/984041457.html >

(2006, 27 de Diciembre) " El escándalo que acabó con la carrera política de Richard Nixon". *El Mundo* [artículo en línea] [Fecha de consulta: 31 de Marzo de 2014]
<http://www.elmundo.es/elmundo/2005/06/01/internacional/1117593594.html >

Collado, A. "Qué es el caso Watergate". [Fecha de consulta: 31 de Marzo de 2014]
< http://historiausa.about.com/od/presid/a/Qu-E-Es-El-Caso-Watergate.htm>

Borja, M. (2012, 29 de Marzo) " Análisis de la Ley Patriota de los Estados Unidos y su repercusión en el ámbito internacional". [Fecha de consulta: 31 de Marzo de 2014]
< http://mensiuris.wordpress.com/2012/03/29/analisis-de-la-ley-patriota-de-los-estados-unidos-y-su-repercusion-en-el-ambito-internacional/>

Steele, C. (2014, 11 de Febrero) "The 10 Most Disturbing Snowden Revelations". *PC Magazine*. [Fecha de consulta: 2 de Abril de 2014]
<http://www.pcmag.com/article2/0,2817,2453128,00.asp>

Appelbaum, J.; Horchert J.; Stöcker C. (2013, 29 de Diciembre) " Shopping for Spy Gear: Catalog Advertises NSA Toolbox". *Spiegel OnLine Internacional*. [Fecha de consulta: 2 de Abril de 2014]
< http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>

Free Snowden in support of Edward Snowden. The Courage Foundation. [Fecha de consulta: 2 de Abril de 2014]
<https://freesnowden.is/revelations/>

The Guardian (2013, 6 de Junio*)."*NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things – video" [vídeo]. *The Guardian* [artículo en línea]. [Fecha de consulta: 2 de Abril de 2014]
<http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>

Rodríguez, G. (2013, 9 de Junio)."Edward Snowden Interview Transcript FULL TEXT: Read the Guardian's Entire Interview With the Man Who Leaked PRISM". [Fecha de consulta: 2 de Abril de 2014]
<http://www.policymic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism>

Greenwald, G.; Poitras, L.; MacAskill, E. (2013, 11 de Septiembre). "NSA shares raw intelligence including Americans' data with Israel". *The Guardian* [artículo en línea]. [Fecha de consulta: 3 de Abril de 2014]
<http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents>

Leslie, T.; Corcoran, M. (2013, 19 de Noviembre). "Explained: Australia's involvement with the NSA, the US spy agency at heart of global scandal". *Abc* [artículo en línea] [Fecha de consulta: 4 de Abril de 2014]
<http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786>

Borger, J. (2013, 1 de Noviembre)."GCHQ and European spy agencies worked together on mass surveillance". *The Guardian* [artículo en línea] [Fecha de consulta: 4 de Abril de 2014]
<http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden>

Weston, G.; Greenwald, G.; Gallagher, R. (2013, 9 de Diciembre).” Snowden document shows Canada set up spy posts for NSA”. *CBC News* [artículo en línea] [Fecha de consulta: 4 de Abril de 2014] <http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886>

Cremer, J. (2013, 4 de Noviembre).” Denmark is one of the NSA's '9-Eyes'”. *The Copenhagen Post* [artículo en línea] [Fecha de consulta: 4 de Abril de 2014] <http://cphpost.dk/news/denmark-is-one-of-the-nsas-9-eyes.7611.html>

Follorou, J. (2013, 29 de Noviembre).” La France, précieux partenaire de l'espionnage de la NSA”. *Le Monde* [artículo en línea] [Fecha de consulta: 4 de Abril de 2014] <http://www.lemonde.fr/technologies/article/2013/11/29/la-france-precieux-partenaire-de-l-espionnage-de-la-nsa_3522653_651865.html>

Fuchs, C.; Goetz, J. ; Obermaier F. (2013, 13 de Septiembre).” Verfassungsschutz beliefert NSA”. [Fecha de consulta: 5 de Abril de 2014] <http://www.sueddeutsche.de/politik/spionage-in-deutschland-verfassungsschutz-beliefert-nsa-1.1770672>

Greenwald, C.; Aranda, G. (2013, 31 de Octubre).” El CNI facilitó el espionaje masivo de EEUU a España”. *El Mundo* [artículo en línea] [Fecha de consulta: 5 de Abril de 2014] <http://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html>

Collado, A. (2013, 31 de Octubre).” El canje de datos CNI-NSA se ciñe a rastreos en "el Sahel y zonas de guerra"”. *El Confidencial* [artículo en línea] [Fecha de consulta: 5 de Abril de 2014] <http://www.elconfidencial.com/espana/2013-10-31/el-canje-de-datos-cni-nsa-se-cine-a-rastreos-en-el-sahel-y-zonas-de-guerra_48451/>

Osborne, L. (2013, 29 de Octubre).” Europeans outraged over NSA spying, threaten action”. *USA Today* [artículo en línea] [Fecha de consulta: 5 de Abril de 2014] <http://www.usatoday.com/story/news/world/2013/10/28/report-nsa-spain/3284609/>

Orange, R. (2013, 19 de Noviembre). “NSA logged 33m calls in Nato ally Norway”. *The Local* [artículo en línea] [Fecha de consulta: 5 de Abril de 2014] <http://www.thelocal.no/20131119/nsa-recorded-m-phone-calls-of-nato-ally-norway>

Rensfeldt, G. (2013, 11 de Diciembre). “FRA has access to controversial surveillance system”. *Sveriges Television* [artículo en línea] [Fecha de consulta: 5 de Abril de 2014] <http://www.svt.se/ug/fra-has-access-to-controversial-surveillance-system>

Derix, S.; Greenwald, G; Modderkolk, H. (2013, 30 de Noviembre). "Dutch intelligence agency AIVD hacks internet forums". *NRC* [artículo en línea] [Fecha de consulta: 5 de Abril de 2014] <*http://www.nrc.nl/nieuws/2013/11/30/dutch-intelligence-agency-aivd-hacks-internet-fora/*>

Dimitri. (2013, 30 de Octubre). "Secrets about NSA's Spy Hub in Geneva". [Fecha de consulta: 5 de Abril de 2014] <http://www.newlyswissed.com/secret-nsa-spy-hub-in-geneva/>

Tubella, P. (2013, 23 de Agosto). "La NSA pagó millones a los gigantes de Internet por colaborar en el espionaje". *El País* [artículo en línea] [Fecha de consulta: 5 de Abril de 2014] <http://internacional.elpais.com/internacional/2013/08/23/actualidad/1377272049_738995.html>

Sánchez, R. (2014, 26 de enero). "Snowden: 'La NSA no busca la seguridad nacional, sino el espionaje industrial'". *El Mundo* [artículo en línea][Fecha de consulta: 5 de Abril de 2014] <http://www.elmundo.es/internacional/2014/01/26/52e559d4e2704edd598b457b.html>

Schlesinger, R. (2013, 8 de Junio). "The Corporate Roots of the NSA Spying Controversy". *US News* [artículo en línea][Fecha de consulta: 5 de Abril de 2014] <http://www.usnews.com/opinion/blogs/robert-schlesinger/2013/06/08/nsa-prism-phone-records-spying-are-built-on-corporate-surveillance>

Auerbach, D. (2014, 8 de Enero). "The NSA Is Bad for Business". [Fecha de consulta: 6 de Abril de 2014] <http://www.slate.com/articles/technology/bitwise/2014/01/google_apple_facebook_and_the_nsa_tech_companies_come_together_to_limit.html>

Kerr, D. (2013, 31 de Octubre). "Apple, Google, Microsoft unite against NSA spying program". [Fecha de consulta: 6 de Abril de 2014] <http://www.cnet.com/news/apple-google-microsoft-unite-against-nsa-spying-program/>

Barrett, B. (2013, 6 de Julio). "What Is PRISM?". [Fecha de consulta: 6 de Abril de 2014] <http://gizmodo.com/what-is-prism-511875267>

MacAskill, E.; Borger, J.; Hopkins, N.; Davies, N.; Ball, J. (2013, 21 de Junio). "GCHQ taps fibre-optic cables for secret access to world's communications". *The Guardian* [artículo en línea] [Fecha de consulta: 6 de Abril de 2014] <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

Timberg, C. (2013, 10 de Julio). "The NSA slide you haven't seen". *The Washington Post* [artículo en línea][Fecha de consulta: 7 de Abril de 2014] <http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html>

(2014, 17 de Enero). "Slides about NSA's Upstream collection". [Fecha de consulta: 7 de Abril de 2014] <http://electrospaces.blogspot.com.es/2014/01/slides-about-nsas-upstream-collection.html>

(2013, 31 de Julio). "XKeyscore presentation from 2008 – read in full". *The Guardian* [artículo en línea] [Fecha de consulta: 7 de Abril de 2014] <http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation>

(2013, 5 de Septiembre). "Secret Documents Reveal N.S.A. Campaign Against Encryption". *The New York Times* [artículo en línea] [Fecha de consulta: 8 de Abril de 2014] <http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=0>

Paganini, P. (2013, 7 de Septiembre). "NSA Bullrun program, encryption and false perception of security". [Fecha de consulta: 9 de Abril de 2014] <http://securityaffairs.co/wordpress/17577/intelligence/nsa-bullrun-program-false-perception-security.html>

Pastor, J. (2013, 6 de Septiembre) "Hacking gubernamental: La NSA y el CGHQ descifran protocolos seguros para espiarlo todo en Internet". [Fecha de consulta: 9 de Abril de 2014] <http://www.xataka.com/otros/hacking-gubernamental-la-nsa-y-el-cghq-descifran-protocolos-seguros-para-espiarlo-todo-en-internet>

(2014, 5 de Abril). "XKeyscore". *Wikipedia* [artículo en línea] [Fecha de consulta: 9 de Abril de 2014] <http://en.wikipedia.org/wiki/XKeyscore>

(2014, 11 de Abril). "Upstream collection". *Wikipedia* [artículo en línea][Fecha de consulta: 12 de Abril de 2014] <http://en.wikipedia.org/wiki/Upstream_collection>

(2014, 11 de Abril). "Bullrun (decryption program)". *Wikipedia* [artículo en línea] [Fecha de consulta: 12 de Abril de 2014] <http://en.wikipedia.org/wiki/Bullrun_%28decryption_program%29>

Casaretto, J. (2013, 6 de Septiembre) "Hacking Bullrun: The NSA Backdoor Anti-Encryption Bug Program That Breaks Most Encryption on the Internet". [Fecha de consulta: 13 de Abril de 2014] <http://siliconangle.com/blog/2013/09/06/bullrun-the-nsa-backdoor-anti-encryption-bug-program-that-breaks-most-encryption-on-the-internet/>

Staff, V. (2013, 17 de Julio) .“Everything you need to know about PRISM”. [Fecha de consulta: 13 de Abril de 2014]
<http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>

“Opt out of global data surveillance programs like PRISM, XKeyscore and Tempora”. [Fecha de consulta: 13 de Abril de 2014]
< https://prism-break.org/en/>

Schoen, S. (2013, 17 de Julio)."Technology to Protect Against Mass Surveillance (Part 1)" [Fecha de consulta: 10 de Mayo de 2014]
<https://www.eff.org/deeplinks/2013/07/technology-protect-against-mass-surveillance-part-1 >

O'Brien, D. (2013, 25 de Octubre). "Ten Steps You Can Take Right Now Against Internet Surveillance" [Fecha de consulta: 10 de Mayo de 2014]
<https://www.eff.org/deeplinks/2013/10/ten-steps-against-surveillance>

"What Can I Do To Protect Myself?”. *Surveillance Self-Defense* [Fecha de consulta: 14 de Mayo de 2014]
<https://ssd.eff.org/wire/protect>

"Essential Online Tools to Protect Yourself from Invasive Government-Corporate". *Emergent Culture* [Fecha de consulta: 14 de Mayo de 2014]
<http://emergent-culture.com/essential-online-tools-to-protect-yourself-from-invasive-government-corporate-surveillance-spying-snowden-manning-prism-nsa-cia-boundless-informant-tempora-police-state>

Schneier, B.(2013, 6 de Septiembre) "NSA surveillance: A guide to staying secure".*The Guardian* [artículo en línea] [Fecha de consulta: 14 de Mayo de 2014]
<http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance>

Maggos, I.(2013, 27 de Octubre) "Against Internet Surveillance"[Fecha de consulta: 14 de Mayo de 2014]
<http://www.terrapapers.com/?p=45180>

Lee, M.(2013, 2 de Julio)."Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance" [Fecha de consulta: 17 de Mayo de 2014]
<https://pressfreedomfoundation.org/encryption-works>

(2014, 25 de Marzo). “End-to-end encryption”. *Wikipedia* [artículo en línea] [Fecha de consulta: 17 de Mayo de 2014]
<http://en.wikipedia.org/wiki/End-to-end_encryption>

"Off-the-Record Messaging Protocol version 3". [Fecha de consulta: 17 de Mayo de 2014]
<https://otr.cypherpunks.ca/Protocol-v3-4.0.0.html>

Crawford, D. (2013, 13 de Junio)."The NSA Prism scandal and how VPN can and cannot help" [Fecha de consulta: 17 de Mayo de 2014]
<https://www.bestvpn.com/blog/6484/the-nsa-prism-scandal-and-how-vpn-can-and-cannot-help/>

Velu, K. (2014, 15 de Enero)." Search the Web Anonymously: 4 Options" [Fecha de consulta: 17 de Mayo de 2014]
<http://www.brighthub.com/internet/google/articles/93816.aspx>

(2014, 19 de Mayo). "OpenVPN". *Wikipedia* [artículo en línea] [Fecha de consulta: 19 de Mayo de 2014]
<http://es.wikipedia.org/wiki/OpenVPN>

Tor Project [Fecha de consulta: 20 de Mayo de 2014]
<https://www.torproject.org/>

"Tor (anonymity network)". *Wikipedia* [artículo en línea] [Fecha de consulta: 20 de Mayo de 2014]
<http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29>

"Tor". *Surveillance Self – Defence* [Fecha de consulta: 20 de Mayo de 2014]
<https://ssd.eff.org/tech/tor>

Zimmermann, P.; Callas, J.; Johnston, A.; Avaya, Ed. (2010, 17 de Junio) "ZRTP: Media Path Key Agreement for Unicast Secure RTP".*IETF* [Fecha de consulta: 20 de Mayo de 2014]
<http://tools.ietf.org/html/draft-zimmermann-avt-zrtp-22>

Ball, J.;Schneier, B.; Greenwald, G. (2013, 4 de Octubre*)."* NSA and GCHQ target Tor network that protects anonymity of web users". *The Guardian* [artículo en línea] [Fecha de consulta: 21 de Mayo de 2014]
<http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption>

Rosenbach, M.; Poitras, L.; Stark, H. (2013, 9 de Septiembre)." iSpy: How the NSA Accesses Smartphone Data". *Spiegel Online* [artículo en línea] [Fecha de consulta: 12 de Junio de 2014]
<http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html>