INFORME 2013

REPORTEROS SIN FRONTERAS
POR LA LIBERTAD DE INFORMACIÓN

ENEMIGOS DE INTERNET

ÍNDICE

INTRODUCCIÓN

"Mi ordenador fue interceptado antes que yo", es el testimonio de un activista sirio detenido y torturado por el régimen de Bachar Al-Assad. Karim Taymour, explica a un periodista de Bloomberg cómo le presentaron, en su interrogatorio, más de 1.000 páginas que detallaban sus conversaciones electrónicas y sus archivos intercambiados por Skype. Sus verdugos sabían manifiestamente tanto de él como si hubiesen estado en su habitación o en su ordenador. La vigilancia en Internet representa un peligro enorme para los periodistas, blogueros, periodistas ciudadanos y defensores de los derechos humanos. En 2011, Wikileaks hacía públicos los "spyfiles" que mostraban la magnitud del mercado de la vigilancia en Internet y el mercado financiero que representa (más de cinco millones de dólares), así como la sofisticación de los productos que maneja.

La vigilancia tradicional no ha desaparecido del todo: la policía continúa vigilando los cibercafés de Eritrea; todavía hay agentes vestidos de civil que persiguen a disidentes vietnamitas; la policía china sigue vigilando el domicilio de Zeng Jinyan o Hu Jia; y las escuchas telefónicas a periodistas han facilitado mucho el trabajo a los servicios de información. Pero, hoy en día, las posibilidades que ofrece la vigilancia en Internet, amplían mucho el campo a los gobiernos.

La edición 2013 del Informe sobre los Enemigos de Internet aborda la vigilancia en la red, en el sentido de la actividad destinada a controlar las voces disidentes y la difusión de informaciones sensibles, una actividad organizada para prevenir toda desestabilización potencial del orden establecido.

El 12 de marzo, Día Mundial Contra la Censura en Internet, se hace pública una primera lista de cinco Estados enemigos de Internet. Son Estados que practican una vigilancia activa e intrusiva y que permite graves violaciones de la libertad de información y de los derechos humanos. Se trata de Siria, China, Irán, Bahréin y Vietnam.

Junto a los países, el Informe publica además una lista de cinco empresas enemigas de Internet, también llamadas "mercenarias de la era digital": Gamma, Trovicor, Hacking Team, Amesys y Blue Coat, que han sido seleccionadas en una lista que se ampliará durante los próximos meses. Sus productos son utilizados

INTRODUCCIÓN

por las autoridades de diversos países para cometer violaciones de derechos humanos y de la libertad de información. Estas empresas no podían egnorar, en el mismo instante en que estas empresas aceptaron comerciar con regímenes autoritarios, que sus productos podían ser utilizados para vigilar a periodistas, disidentes e internautas. La imposibilidad de estas propias empresas de seguir la pista a sus productos vendidos a regímenes autoritarios demuestra hasta qué punto no son conscientes del riesgo de utilización derivado de sus tecnologías y de la vulnerabilidad de los defensores de los derechos humanos.

Las encuestas realizadas por Bloomberg, el Wall Street Journal y el Citizen Lab, de la Universidad de Toronto, han revelado que las tecnologías para vigilar Internet utilizadas contra disidentes y activistas de derechos humanos, en países como Egipto, Bahréin o Libia provenían de empresas occidentales.

A lo largo del informe se exponen una serie de productos que ayudan a vigilar Internet: escuchas a gran escala para vigilar la red en su conjunto y "spywares". Estos "spywares" se utilizan para espiar el contenido de discos duros, recuperar contraseñas, acceder al contenido de mensajes electrónicos o espiar comunicaciones de VOIP. Pueden ser instalados directamente en los ordenadores, o por la red de Internet, a través de falsas actualizaciones o de archivos adjuntos en un correo electrónico, sin que el usuario se de cuenta. El uso civil de este tipo de programas está limitado, pero algunos fabricantes proveen directamente de ellos a actores estatales, como servicios secretos y servicios de seguridad. Otros no dudan en hacer publicidad de sus capacidades para vigilar a oponentes políticos y los regímenes autoritarios utilizan este sistema para espiar a periodistas y sus fuentes.

Algunas tecnologías permiten además un doble uso: ser utilizadas con fines legítimos de lucha contra los delitos informáticos, o ser utilizadas como terribles herramientas de censura y vigilancia contra los defensores de los derechos humanos e informadores. La falta de regulación del comercio de estas "armas digitales" permite a los gobiernos autoritarios identificar a periodistas ciudadanos y encarcelarlos.

Reporteros Sin Fronteras lleva tiempo exigiendo un control de la exportación de estas tec-

nologías a países que no respetan derechos fundamentales. Un control que no debe quedar en manos exclusivas del sector privado, y que deben ser competencia de los legisladores. La Unión Europea y Estados unidos ya han prohibido la exportación de sistemas de vigilancia a Irán y Siria, una decisión loable que no debería ser un caso aislado. Los Estados europeos deben adoptar una legislación que controle la exportación de tecnologías de vigilancia en Internet. La administración Obama debe adoptar igualmente este tipo de legislación, como la Global Online Freedom Act (GOFA).

Existen precedentese en las negociaciones entre gobiernos, que llevaron al acuerdo de Wassennaar, concluido en julio de 1996, que buscaba promover "la transparencia y una mayor responsabilidad en los intercambios de armas y de bienes con doble uso a fin de prevenir acumulaciones desestabilizadoras". Un acuerdo firmado en la actualidad por 40 países.

Las democracias parecen ceder a las voces que reclaman seguridad en Internet y vigilancia a toda costa, como lo demuestra la multiplicación de proyectos y propuestas del leyes potencialmente liberticidas que permitirían la instalación de una vigilancia generalizada. Ejemplo de ellos son la FISAA y CISPA, en Estados Unidos, la British Communication Data Bill, en Reino Unido, la Wetgeving Bestrijding Cybercrime, en los Países Bajos, y tantos textos que sacrifican la libertad de expresión en Internet, alegando luchar contra los delitos informáticos. El hecho de que países tradicionalmente defensores de los derechos humanos adopten este tipo de legislaciones da argumentos a los dirigentes de países represivos para dotarse de un arsenal legislativo con el que acallar a su disidencia. El modelo de Internet tal como fue concebido por sus fundadores, un espacio de intercambio y de libertades que trasciende las fronteras, está contantemente puesto en causa por la aceleración de la censura en Internet y el desarrollo de la vigilancia en la red. Más aún si Internet se ve, además, afectada por las luchas de poder entre distintos Estados. La generalización de la vigilancia es uno de los mayores objetivos de los que luchan por controlar Internet. Con ocasión de la Conferencia Mundial de las Telecomunicaciones de Dubai, en diciembre de 2012, China sostuvo una propuesta destinada a extender de manera drástica el control de la ITU sobre Inernet. China tenía el apoyo de Rusia, Arabia Saudí , Sudán

INTRODUCCIÓN

y Argelia para discutir el papel de la ICANN en la atribución de los nombres de los dominios; de las direcciones IP; de la protección de "la seguridad física y operacional de las redes"; y de la utilización del DPI en las redes de nueva generación.

Una ecuación complicada para los informadores, necesitados por una parte de protección personal y de seguridad para sus fuentes, y, por otra, necesitados también de recoger y hacer circular la información. A día de hoy, la protección de las fuentes no se refiere solamente a la ética de los periodistas, sino que depende cada vez más del uso de su ordenador, como apunta el especialista de seguridad en Internet Chris Soghoian, en un editorial publicado en el New York Times.

Antes de partir al terreno, el reportero de guerra, si es cuidadoso con su seguridad física, se provee de un casco y un chaleco antibalas. De la misma forma, todo periodista debería proveerse de un "kit de supervivencia numérica", en el momento que almacene o intercambie informaciones sensibles en Internet, ya sea con su ordenador o su teléfono móvil. Este kit, desarrollado progresivamente por Reporteros Sin Fronteras, destaca, en primer lugar, la necesidad de limpiar sus documentos, y explica cómo utilizar la red Tor o redes privadas virtuales, VPNs, para conseguir el anonimato de sus comunicaciones. También da consejos para hacer más seguras las comunicaciones y los datos sobre los terminales móviles, etcétera.

Los periodistas e internautas deben aprender a calcular mejor los riesgos potenciales de la vigilancia y el tipo de datos o de comunicaciones que hay que proteger, a fin de encontrar la solución adaptada al uso que hacen de Internet. Frente a la sofisticación de los medios desplegados por los censores y servicios de información, el ingenio de los informadores y de los hacker activistas está puesto a prueba constantemente. De quién venza este pulso depende el porvenir de la libertad de informar. Un combate sin bombas, sin barrotes de prisiones, pero donde, si no se tiene cuidado, los enemigos de la realidad y de la verdad podrán imponer un dominio absoluto.

BAHRÉIN

Bahrein es uno de los países de Oriente Medio con mayor cobertura de Internet. Su tasa de usuarios alcanza al 77% de la población. Tiene una velocidad de conexión relativamente alta (entre 512 KB y 20 GB, dependiendo de la región) y un alto porcentaje de proveedores de servicios de Internet (ISP) por habitante: 23 para un total de 1.250.000 habitantes. Batelco, dirigido por la familia real bahrení, es, de lejos, el más importante.

Desde el inicio de las revueltas populares del año 2011, Internet fue una gran herramienta de comunicación e información en el país. Los activistas tuevieron a su disposición una red de calidad para compartir ideas y documentos a través de los medios de comunicación en Internet, blogs y redes sociales. Según la última encuesta de la Social Media Club, el número de twitteros creció un 40% la segunda mitad de 2012.

Vigilancia en la red

Si Bahréin es uno de los países mejor conectados a Internet del Golfo, también es uno de los que más ha desarrollado el filtrado de contenidos en la red del mundo. La familia real está representada en todas las administraciones de investigación, y dispone de herramientas avanzadas para vigilar a sus ciudadanos. En 2012, Bahrein entró en la lista de países "Enemigos de Internet", elaborada anualmente por Reporteros Sin Fronteras, y la situación no ha mejorado desde las protestas populares de febrero de 2011, inspiradas en las revueltas de Túnez y Egipto.

Una gran comunidad de activistas organizados, pero controlados

Un importante número de contenidos están filtrados y, en teoría, inaccesibles para el público de Internet. Por un lado los considerados "pornográficos", pero también, y sobre todo, las opiniones políticas y religiosas contrarias al régimen. Hay formas de eludir la censura, pero las comunicaciones relativas a la familia real o a las minorías chiíes están muy reguladas.

Las actividades en la red de disidentes e informadores están muy vigiladas, y, según Reda Al-Fardan, miembro de la ONG Bahrein Watch, los activistas bahreníes están muy organizados, pero también muy expuestos: "el número de ataques informáticos ha crecido desde marzo de 2012", advierte.

BAHRÉIN

Se han identificado dos tipos de ataques informáticos:

• la instalación de "malwere" (o código "maligno"), mediante elementos adjuntos a los correos electrónicos.

• y la obtención de direcciones IP.

La propagación del "malwere" es cada vez más perniciosa. "Los responsables de estos ataques cada ves son más inteligentes y utilizan hasta alusiones a la libertad de prensa o la defensa de los derechos humanos", afirma Reda Al-Fardan. El Citizen Lab, un centro de investigación vinculado a la Universidad de Toronto, publicó un informe, en julio de 2012, sobre Bahréin, donde detallaba la naturaleza y los programas utilizados en estos ataques informáticos. En dicho informe se mostraba, por ejemplo, un intento de "phishing" generalizado:

El remitente parecía ser la corresponsal de Al-Jazeera, Melissa Chan, y el asunto, los malos tratos recibidos en la cárcel por el director del Centro de Bahréin para los Derechos Humanos, Nabeel Rajab. El informe del Citizen Lab detallaba también un "malwere" enviado por la periodista, escritora y activista bahreiní, Ala'a Shehabi, a Silver Vernon, periodista de Bloomberg. Se ha comprobado que la dirección IP del remitente de este "malware" corresponde a un sitio de Batelco, el principal proveedor de acceso a Internet de Bahréin y propiedad de la familia real.

Pirateo de direcciones IP

El pirateo de cuentas de Twitter y Facebook es frecuente en Bahréin. Siguen un *modus operandi* clásico: la creación de una cuenta falsa que imita la cuenta de los disidentes. Si algún disidente real pincha en alguno de sus enlaces, el "malwere" registra su dirección IP y toda la información de su cuenta. Según la organización Bahrain Watch, la obtención de IPs permite a las autoridades, por ejemplo, desenmascarar una cuenta anónima, como la de los activistas de twitter, desde teléfonos sin VPNs ni Tor u otra herramienta de anonimato. Una vez obtenida la dirección IP basta con buscar en los archivos de la empresa de telefonía móvil, donde se conoce a cada cliente por la IP que utiliza. La red de esta persona recibirá todos los enlaces ya adulterados y así sucesivamente.

Según algunas fuentes, los ataques provienen directamente del gobierno y algunos disiden-

BAHRÉIN

tes han llegado a ser detenidos por las autoridades inmediatamente después de pinchar en estos enlaces.

Interrogatorios y contraseñas

El informe de la Comisión Independiente de Bahréin ha revelado que los disidentes detenidos fueron obligados a identificar a sus contactos en Facebook y Twitter, y a explicar por qué pertenecían a estos grupos, lo que pone en evidencia la estrecha vigilancia de las actividades en Internet de los ciudadanos bahreníes. Tampoco los opositores políticos pueden navegar libremente por la web. Según la organización Bahrain Watch, también están estrechamente controlados.

Una familia real omnipresente

La familia real controla todas las instituciones de difusión y de vigilancia y control de Internet, como Batelco, el proveedor líder de acceso a Internet:

• La Autoridad de Asuntos de Información (IAA) -nombre utilizado por el Ministerio de Información- encabezada por el Ministro de Estado y miembro de la familia real, Fawaz bin Mohammed Al Khalifa, es acusada con frecuencia de censurar a la prensa del país, especialmente desde las protestas de febrero de 2011. La IAA controla los órganos oficiales del gobierno -la agencia de noticias, Bahrein Radio y Television Corporation- y vigila de cerca al único periódico independiente del país, Al-Wasat, además de vigilar a los periodistas y los residentes extranjeros.

• La Organización Central de la informática y las Comunicaciones (más conocida por las siglas COI), está dirigida por otro miembro de la familia real, Salman Mohammed Al-Khalifa. El COI controla Internet en el país, sus sistemas y sus datos. Fue originalmente creado para ser una base de datos de los ciudadanos, pero ha ido ampliando sus poderes a base de reales decretos. En la actualidad tiene autoridad sobre los ISP, y puede eliminar su licencia en cualquier momento, además de acceder y controlar todo su tráfico. Puede acceder a datos de identificación y de uso de Internet de los ciudadanos sin el control de una autoridad independiente y es la principal red de vigilancia del país. Según el Citizen Lab, el COI tiene un dispositivo DPI (ver más abajo) que permite

BAHRÉIN

interceptar las comunicaciones de los ciudadanos. Desde 2012, el organismo está está bajo la autoridad del Ministerio del Interior, dirigido por un miembro de la familia real, Rashid bin Abdulla.

• El Ministerio del Interior (MOI): Además de controlar directamente al COI, el MOI ha creado otro cuerpo para luchar contra la delincuencia informática: La Dirección de Lucha Contra la Corrupción y la Seguridad Electrónica y Económica. Fundada en septiembre de 2012, esta unidad pide a los ciudadanos que denuncien cualquier "campaña de difamación en Internet que pretenda empañar la reputación de los símbolos nacionales y las principales figuras públicas". Alegando luchar contra el "delito de difamación", esta iniciativa ha llevado a la detención, en un solo mes desde que fue creada, de cuatro personas por "mal uso de las redes sociales".

• La Autoridad Reguladora de las Telecomunicaciones (TRA), dirigida por Mohamed Ahmed Al-Amer y Hamed bin Mohammed bin Hamed Al-Khalifa, es responsable del cierre, en 2010 y 2011, de webs como VoIP y Seefcall NonoTalk, considerada ilegal en Bahréin. Este organismo se asegura de que los proveedores de servicios de Internet en el país actualicen las listas negras que elabora el COI.

• El Aparato de la Seguridad Nacional (NSA). La agencia de inteligencia, encabezada por Adel bin Khalifa bin Hamad Al-Fadhel, vigila activamente a los disidentes y opositores políticos, entre otros medios, a través de sus perfiles en redes sociales. Desde 2010, la NSA ha aumentado su poder y se han dado casos de tortura, incluida la de Karim Fakhrawi, fundador y miembro del consejo del periódico *Al-Wasat*, y del bloguero Zakariya Rashid Hassan.

• La Autoridad del "E-gobierno" (EGA). En su deseo de sus digitalizar todas las actividades, el gobierno de Bahréin ha creado el EGA, cuyo objetivo velado pretende recuperar tantos datos como sea posible de los ciudadanos del reino. Por iniciativa de la COI (entonces dirigido por Ahmed Bin Khalifa Al-Atteyatallah), el EGA ha puesto en marcha una campaña de identificación en Internet (Marco Nacional de Autentifición) para "facilitar el acceso a los usuarios de los servicios de Internet". Una iniciativa particularmente preocupante, dada la omnipresencia de las estructuras de la familia real

BAHRÉIN

en la gestión de las telecomunicaciones y la vigilancia del país.

Un arsenal tecnológico de vigilancia

Bahréin posee los últimos equipos de vigilancia y software del mercado. El gobierno de Bahérin puede hacer un seguimiento de la red a todos los niveles.

• Blue Coat: El último informe de Citizen Lab, titulado "Planet Blue Coat" habla del "PacketShaper" una herramienta DPI, producida por la compañía Blue Coat, que permite reconocer y analizar el tráfico de Internet con el fin de bloquear el acceso a ciertos contenidos. Según uno de los autores de este informe, la Organización Central de la informática y las Comunicaciones (COI) de Bahréin ha instalado esta herramienta en sus locales desde donde gestiona toda la red del país.

• Gamma / FinFisher: El Citizen Lab y Bahrain Watch también han demostrado la utilización de un producto de la firma Gamma en Bahréin: FinSpy, de FinFisher. Los productos de FinFisher pueden llegar a controlar todos los ordenadores, webcams y pantallas, registrar todas las veces que se pulsa el teclado, e incluso seguir conversaciones de Skype en teléfonos móviles. Gamma se defiende diciendo que uno de sus productos FinSpy que se utiliza en Bahréin fue robado durante una manifestación. Si resulta sorprendente que una empresa especializada en seguridad informática como Gamma haya extraviado uno de sus propios productos de seguridad durante una manifestación, lo es aún más que los productos FinFisher encontrados en Bahréin por Citizen Lab hayan sido actualizados. De hecho, según Bill Marczak, miembro de Bahrain Watch y editor del informe de Citizen Lab sobre Bahréin, las versiones del FinSpy descubierto en Bahréin en marzo de 2012, son del modelo 1,4, después de haber descubierto con anterioridad un modelo del 4.0.

• Trovicor: Según las fuentes de RSF, Bahréin tiene, desde finales de 1990, productos de Trovicor, que, como los FinFisher, permiten vigilar las conversaciones en Internet, teléfonos móviles y SMS. Varias empresas, como Nokia Siemens Networks, recibieron la orden de dejar de vender sus productos a Bahréin. El centro de datos de Nokia Siemens Network fue comprado por...Trovicor. Una venta que permitió la vigilancia, detención y tortura de opositores.

BAHRÉIN

• Además también se ha utilizado en Bahréin el software de la estadounidense McAfee, SmartFilter, en 2011, junto a otras herramientas DPI.

Violaciones a la libertad de información

Durante tres años, incluso antes del movimiento de protesta popular de la Primavera Árabe, Reporteros Sin Fronteras ya había observado un resurgimiento de graves violaciones de la libertad de información en Bahréin. El país es un ejemplo de represión, capaz de llevar a cabo un auténtico apagón informativo gracias a su impresionante arsenal de medidas represivas y de vigilancia que aplica a los medios de comunicación extranjeros, a los defensores de los derechos humanos, mediante la detención de blogueros e internautas, o llevando ante la justicia a activistas de la libertad de expresión, o haciendo campañas de difamación contra ellos.

En la actualidad hay varios periodistas, internautas y defensores de los derechos humanos encarcelados en Bahréin, o con riesgo de estarlo, por un publicar un artículo, una foto, o una simple actualización de su estado de Facebook. El papel de estos informadores es más importante si cabe ante el elevado número de periodistas extranjeros que no pueden entrar al territorio bahrení. A finales de 2012, Asem Al-Ghamedi, de *Al-Al-Jazeera*, Nicholas Kristof, del *New York Times* y corresponsal del *Frankfurter Allgemeine Zeitung*, vieron denegado su acceso al país por "defectos de procedimiento" en la obtención de sus visados.

Informadores encarcelados o en riesgo de estarlo

(Actualización a 1 de marzo de 2013)

• Abduljalil Al-Singace, defensor de los derechos humanos y bloguero. Es uno de los 21 condenados, el 22 de junio 2011, por "pertenencia a una organización terrorista" e "intentos de derrocar al régimen ". Se han agotados todos los recursos a su sentencia y cumple en la actualidad un cadena perpetua.

• Ali Abdulemam, juzgado sin su propia presencia en el tribunal. Fue condenado a 15 años de cárcel. Tras la publicación del informe Bas-

BAHRÉIN

siouni, las autoridades judiciales bahreníes ordenaron, el 30 de abril de 2012, la celebración de un nuevo juicio, civil en esta ocasión, ante el Tribunal de Apelación.

• Ahmed Humaidan, reportero gráfico, ganador de 143 premios internacionales, lleva detenido desde el 29 de diciembre de 2012 por documentar violaciones de los derechos humanos. Según su familia, ha sido obejeto de malos tratos y torturas durante su detención. Se le acusa de haber participado en un ataque contra una comisaría, en 2011, mientras cubría los hechos.

• Hassan Salman Al-Ma'atooq, fotógrafo encarcelado desde marzo de 2011. Fue acusado de "fabricar imágenes de heridos y difundir imágenes y noticias falsas".

Entre los defensores de los derechos humanos y los informadores también víctimas de la represión, se encuantran Nabeel Rajab, presidente del Centro de Bahréin de Derechos Humanos (BCHR) y Said Yousif Al-Muhafdha, vicepresidente del mismo centro.

Internautas víctimas de torturas

• El periodista ciudadano Ahmed Ismail Hussain fue asesinado mientras cubría una manifestación pacífica, el 31 de marzo 2012. Sus asesinos no han sido detenidos hasta la fecha.

• Karim Fakhrawi, fundador y miembro de la directiva del periódico *Al-Wasat*, y el blogueiro Zakariya Rashid Hassan, murieron mientras estaban detenidos, víctimas de torturas. La justicia de Barhéin no ha investigado a ninguna de las personas implicadas en su muerte.

Otros dos ejemplos demostraron, a finales del 2012 la actitud del sistema judicial bahrení ante estos abusos contra los profesionales de la información.

• La periodista Reen Jalifa fue acusada, y condenada, de agredir a tres médicos durante una conferencia de prensa, en julio de 2011. En realidad ella había sido la agredida.

• El Tribunal Supremo decidió absolver a la teniente Sarah Al-Moosa, acusada de torturar en prisión a la periodista Saeed Nazeeha. Tras esta sentencia, Reporteros Sin Fronteras re-

BAHRÉIN

cordó el informe del 23 de octubre de 2012, del Relator Especial de Naciones Unidas sobre la independencia de jueces y abogados en la impunidad de los actos violentos contra los periodistas en Bahréin.

Soluciones técnicas

Los "spyware" se utilizan ampliamente en Bahrein. "FinFicher" rara vez es detectado por los antivirus, por lo que la única manera efectiva de protegerse contra estos programas es tomar precauciones de antemano para evitar la infección de su ordenador o teléfono móvil.

• No instale ningún software recibido por correo electrónico.

• No instale ningún software, excepto los recogidos en un sitio https. El riesgo de "phishing" (robo de identidad) se reduce con los certificados que garantizan la identidad de un sitio https.

• No instale ningún software de una fuente con la que no esté familiarizado, incluso si la instalación se la recomienda una ventana emergente.

• Haga cambios sistemáticos a su sistema operativo y al software que instala.

• No utilice Internet Explorer para navegar. Es el navegador más utilizado, blanco de la mayoría ataques de piratas informáticos. Es prefiere el Firefox o Chrome.

Otro tema importante en materia de seguridad, es la protección del anonimato en la red. Muchos disidentes que "twitteaban" anónimamente fueron detenidos después de pinchar en enlaces que redireccionaban a una página donde se obtenía la dirección IP de sus visitantes. El uso de una VPN o Tor ayuda a protegerse de este peligro.

Algunos nombres de proveedores de soluciones VPN, son Astrill VPN, Pure VPN o HMA VPN, por ejemplo.

El Guardian Proyect ofrece una gama de programas para preservar su anonimato y privacidad al usar un teléfono con Android, como Orbot, una versión de Tor para teléfonos móviles.

La ONG Access Now ha publicado una guía práctica sobre protección de datos y comuni-

BAHRÉIN

caciones destinada a los usuarios de Oriente Medio, que tiene una sección especialmente dedicada a los teléfonos móviles.

Por último, existe sistema operativo diseñado para proteger el anonimato de sus usuarios: Tails, un sistema que permite el uso de Internet de forma anónima casi en cualquier ordenador sin dejar rastro de las acciones realizadas.

CHINA

El Partico Comunista chino está en la cabeza de uno de los principales imperios numéricos del mundo, si no el mayor. Los puntos de acceso a Internet son propiedad exclusiva del Estado que, con frecuencia, representa al Partido. Los particulares y las empresas tienen la obligación de alquilar su ancho de banda al Estado chino o a una empresa controlada por él. Las cuatro redes nacionales CTNET, Chinanet, Cernet y CHINAGBN, representan la espina dorsal de Internet. En 2008, una reestructuración de la red permitió la aparición de tres grandes proveedores de acceso nacional, China Telecom, China Unicom y China Mobile, controladas mayoritariamente por el Estado chino. El acceso público a Internet se delega a compañías regionales.

En un informe de enero de 2013, el sitio oficial Chine Internet Network Information Center (CNNIC) cifra una tasa de utilización de Internet del 42,1% de la población. Según él, China tiene 564 millones de interneutas, de los que 277 millones acceden a Internet vía un terminal móvil.

Facebook cuenta con 63,5 millones de usuarios, un número multiplicado por 8 estos dos últimos años. Twitter reúne a 35 millones, o sea, tres veces más que en 2009. La red social China Weibo habría igualmente multiplicado por tres el número estimado de sus usuarios, para alcanzar la cifra de 504 millones.

El coste de acceso de una conexión DSL, con un trafico de 1MBit, ronda, según las provincias, entre 10 y 20 dólares al mes.

Vigilancia en Internet

Hay muchos departamentos estatales implicados en la censura y la vigilancia de la red:

• La Oficina de Internet y el Centro de Estudio de la Opinión Pública de la Oficina de la Información del Consejo de Estado (equivalente al gobierno);

• La Oficina de Internet y la Oficina de la Información y de la Opinión Pública del Departamento de Publicidad (antiguo departamento de la propaganda);

• El Ministerio de la Industria de la Información (MII);

CHINA

• La Oficina de Vigilancia y de Seguridad de las Informaciones en Internet del Ministerio de la Seguridad Pública;

• y el Centro de Registro de las Informaciones Ilegales e Inconvenientes sobre Internet del Ministerio de la Industria de la Información (MII).

Los dos últimos órganos citados gestionan los asuntos relacionados con la pornografía, la violencia y el fraude electrónico. El MII no participa directamente en el control de Internet. Los órganos influyentes son la Oficina de la Información, el Consejo de Estado, y el Departamento de Publicidad.

La Gran Muralla Electrónica

El conjunto de herramientas utilizadas para filtrar y vigilar Internet en China se conoce con el nombre de "Gran Muralla Electrónica de China". Lanzada en 2003, este sistema permite filtrar el acceso a las webs extranjeras. Más allá de las reglas clásicas de seguimiento permanente que permiten bloquear el acceso a una dirección IP o a un dominio, la Gran Muralla Electrónica de China utiliza masivamente las tecnologías DPI para la detección y el bloqueo de palabras clave.

Según el informe Plane Bluecoat, del centro de investigación ligado a la Universidad de Toronto, Citizen Lab, al menos tres servidores Bluecoat se utilizan en la red de proveedores de acceso China Net (controlada por el Estado chino) en la provincia de Sichuan. Su presencia ha sido detectada a finales de 2012. Bluecoat es una sociedad especializada en la vigilancia de redes, y los servidores identificados en China son de tipo PacketShaper. Permiten identificar y controlar el tráfico bloqueando ciertos flujos o contenidos considerados indeseables.

Cómo evadir la censura

Hay numerosos medios -proxi, VPN, Tor- que permiten escapar a este sistema de vigilancia, pero poco utilizados a escala de la población china.

Los VPN de pago chinos no son muy populares. Necesitan la utilización de una tarjeta de crédito, un medio de identificación muy eficaz. Sabiendo que toda sociedad que comercializa un servicio de VPN en china debe registrarse en el

CHINA

Ministario de la Industria y las Tecnologías de la Información, su uso hace aún más peligroso.

Las herramientas de evasión de la censura gratuitas, como Tor o Freegat, son blanco constante de las autoridades, lo que las transforma en lentas e inestables. Su utilización está por tanto lejos de ser sistemática. Quedan las soluciones proporcionadas por sociedades situadas fuera de China. Constituyen hasta aquí una alternativa para los ciudadanos chinos.

La puesta al día de la Gran Muralla

Con motivo del XVIII Congreso del Partido Comunista, en noviembre de 2012, las autoridades chinas procedieron a una puesta al día de la gran muralla electrónica, con el objetivo de imponer un bloqueo informativo: Las soluciones VPN proporcionadas por empresas extranjeras fueron neutralizadas. Los principales usuarios de VPNs en el extranjero vieron bloqueadas sus conexiones.

La Gran Muralla Electrónica de China tiene la capacidad de bloquear dinámicamente las conexiones cifradas. Uno de los principales proveedores de acceso a Internet del país, China Unicorn, pone automáticamente fin a toda conexión en cuanto el contenido transmitido está cifrado.

Hasta hoy sólo los servicios VPN de la sociedad Astril parecen estar ayudando a permitir a los ciudadanos chinos pasar a través de la Gran Muralla Electrónica y mantener su anonimato en Internet. Los otros grandes proveedores VPN (Witopia, StrongVPN, AirVPN, eyc.) están bloqueados.

La utilización de VPNs permite, no solamente evadir el bloqueo impuesto por las autoridades, sino también ocultar la dirección IP y cifrar las comunicaciones sobre Internet. La puesta al día de la Gran Muralla Electrónica de China y el bloqueo de los medios de cifrado, exponen a las comunicaciones de los periodistas e internautas chinos al sistema de vigilancia de las autoridades.

Dispositvo de vigilancia integral

Pero el dispositivo de vigilancia utilizado en China no se limita a la Gran Muralla Electrónica, a la identificación y al bloqueo de las comunicaciones que entran y salen. Los medios de

CHINA

vigilancia están inegrados en las redes sociales, chats y VoIP. Las empresas privadas tienen un ancargo directo de las autoridades chinas de asegurar la vigilancia de su red a fin de impdir la difusión de mensajes prohibidos.

El software QQ,, de la empresa Tencent, permite a las autoridades vigilar con precisión los intercambios de todos los interneutas, buscando ciertas palabras clave o expresiones. Se puede identificar al autor de cada mensaje gracias al núero de utilizador del software. El sitio de microbloging QQ es en sí mismo un gigantesco caballo de Troya.

Una nueva legislación, impuesta desde marzo de 2012, obliga a todo nuevo usuario de microblogin a registrarse bajo su verdadero nombre y a dar su número de teléfono. A fin de forzar a los usuarios ya existentes a someterse a este control, en el marco de la evolución de sus condiciones generales de utilización, el sitio Sina Waibo ha sacado al mercado un permiso con puntos: Cada usuario parte con 80 puntos y cada infracción supone una retirada de un número de puntos preestablecido. Cuando llegan a cero se cierra la cuenta. Los usuarios con pocos puntos pueden volver a ganarlos si no cometen infracciones durante dos meses o si participan en actividades no especificadas de promoción.

En febrero de 2013, la aplicación móvil de envio de mensajes de texto y voz WeChat, muy popular, ha modoficado sus condiciones de utilización. Su usuarios, entre los cuales hay numerosas sociedades y celebridades, deben proporcionar a partir de ahora un número de carné nacional de identidad, un número de móvil y enviar una fotocopia de su DNI.

Para perfeccionar el control y cortar cualquier intento de anonimato, el Congreso Nacional del Pueblo Chino adoptó, en diciembre de 2012, una medida que obliga a los ciudadanos que deseen suscribirse a Internet o a un servicio móvil a proporcionar su verdadera identidad.

Tom Skype

Las redes sociales no son las únicas afectadas por estas medidas de control. Skype, una de las herramientas de telefonía en Internet más populares del mundo, está bajo estrecha vigilancia. En China los servicios de Skype se distribuyen de una forma compartida con la em-

CHINA

presa local Tom. La versión china de Skype, denominada Tom Skype, difiere ligeramente de las versiones de los otros países.

A fin de adapatarse a las restricciones impuestas por el gobierno chino, el software Tom Skype está equipado con un filtro automático. Cuando ciertas palabras clave son detectadas, éste es bloqueado. Y, según un informe del Open Net Intitative Asie, pasa a ser almacenado en un servidor. La vigilancia y la interceptación de los mensajes instantáneos en Tom Skype no se basa sólo en las palabras clave, sino también en el nombre de ciertos usuarios. El informe de la Open Net Intiative Asie comprueba conversaciones banales almacenadas en servidores. El nombre del expedidor o del destinatario constituría un criterio suficiente para la intercepción y el almacenamiento de sus conversaciones.

Sin la utilización de medios de evasión de la censura de tipo Tor o VPN, el sitio oficial de Skype reenvía hacia el sitio Tom Skype. Siendo los dos sitios semejantes, algunos usuarios de Tom Skype no saben probablemente que utilizan una versión modificada de Skype y que su seguridad está potencialmente amenazada.

En enero de 2013, Reporteros Sin Fronteras firmó con otras ONGs una carta abierta pidiendo a Skype precisiones sobre sus relaciones con la sociedad china Tom Skype, tanto sobre los mecanismos de vigilancia, como de censura, implantados en sus softwares.

Petición a empresas extranjeras

El Comité para la Protección de la Calidad de las Marcas es un grupo que representa a varias multinacionales en China, tales como Apple, Nokia, Toyota, Audi, etc. Este comité envió un mensaje a sus 216 miembros informándoles de las inquietudes de las autoridades chinas sobre la utilización de VPNs por parte de estas multinacionales, que permiten a sus empleados intercambiar información sin que el contenido de sus comunicaciones pueda ser interceptado por la Gran Muralla Electrónica. El comunicado informaba de una posible visita de la policía china a cualquiera de estas empresas. En Pekin, Hebei y Shandong, la policía ya habría pedido a algunos de ellos instalar un software que permitiese vigilar su red. De negarse, las autoridades habrían amenazado con cortar el acceso aInternet de estas empresas.

CHINA

Daños colaterales

Uno de los frenos en la puesta a punto de herramientas de vigilancia y de control de la red en China es el impacto económico de estas medidas para las sociedades chinas y extranjeras. En la era de Internet, la vigilancia tiene efectivamente un coste que repercute en la competitividad de las empresas.

Los dirigentes de los portales de Internet están frustrados por la energía y el tiempo invertidos en implantar mecanismos de censura. Por ejemplo Tencent, el gigante chino de Internet, que debe invertir gran cantidad de recursos para implantar sus mecanismos de censura en su servicio de chat WeChat. En la última puesta a punto de la Gran Muralla Electrónica y el bloqueo sistemático de las conexiones cifradas, numerosas sociedades extranjeras implantadas en China han recurrido a servicios de VPN para acceder a sus datos situados fuera del país, por lo que han sido penalizadas.

Uno de los episodios recientes que demuestra los limites económicos del sistema de censura y de control de la red china se refiere a la plataforma GitHub. GitHub alberga softwares "open source" y numerosas bibliotecas de códigos indispensables para gran cantidad de desarrollos informáticos. Las autoridaes chinas han intentado bloquear el acceso a GitHub, pero GitHup utiliza el protocolo https, impidiendo así a las autoridades chinas bloquear únicamente la página que albergaba los nombres de usuarios de la Gran Muralla. La otra opción de las autoridades chinas era bloquear completamente el sitio. Pero este sito y las numerosas lineas de código que alberga son indispensables para las empresas chinas que trabajan en las nuevas tecnologías y no se hubiese podido superar un bloqueo completo. La única herramienta que permite solucionar este problema es el ataque "Man in the Middle", un ataque que consiste en hacerse pasar por una autoriad de certificación. En tercero puede colocarse entre el sitio https y el internauta e interceptar las conexiones cifradas. El ataque, sin emabrgo, no es transparente y la mayor parte de los navegadores (firefox y chrome) tienen alertas de seguridad que previenen al usuario. Pero las autoridades chinas han optado por esta solución, y, el 26 de enero de 2013, los internutas chinos que se conectaron a GitHub recibieron una alerta de seguridad informándoles que un tercero se hacía pasar por el sitio. El ataque

CHINA

"Man in the Middle" de las autoridades chinas no duró más que una hora y se mostró muy fácil de identificar. Sin embargo, durante esta hora, los internautas que hayan ignorado las alertas de sus navegadores, han podido ser localizados y registradas su IP y contraseñas.

Vigilancia interna y externa

China no ha dudado en extender su perímetro de vigilancia más allá de sus fronteras. El 30 de enero de 2013, el *New York Times* reveló ser blanco de ataques provenientes del gobierno chino. Las primeras intrusiones habrían tenido lugar el 13 de setiembre de 2012, cuando el periódico estaba a punto de publicar su reportaje sobre la fortuna amasada por los familiares del Primer Ministro saliente, Wen Jiabao. Según el periódico estos ataques tenían por objeto identificar las fuentes del periódico sobre la corrupción del entorno del Primer Ministro.

El *Wall Streat Journal* y la *CNN* afirman también haber sido blanco de ataques provenientes de China. En febrero, Twitter reveló que las cuentas de 250.000 usuarios habían sido víctimas de ataques infromáticos similares a las denunciadas por el *New York Times* e igualmente provenientes de China.

Mandiant, la sociedad de seguridad informática que asegura la red del *New York Times*, afirma que los ataques emanan de un grupo de hackers bautizado como "advanced persistant theat 1". Según un informe publicado por la misma empresa, este grupo está localizado en un edificio de un barrio de Shangaï y contaría con miles de empleados. Estarían directamente mantenidos por el gobierno chino y constituirían una filial del Ejército de Liberación del Pueblo. Si no se duda de la realidad y del origen de los ataques contra el *New York Times*, el *Whasington Post* y Twitter, la polémica suscitada por el informe de Mandiant (que tiene como cliente al gobierno estadounidense), ha supuesto para esta sociedad una exposición mediática inesperada. El límite entre una operación de comunicación exitosa y un informe circunstancial es difícil de explicar.

CHINA

Violaciones a la libertad de información

China es la mayor cárcel del mundo de informadores, con 30 periodistas y 69 internautas detenidos en la actualidad. Entre ellos se encuantran algunos casos emblemáticos de la represión, que conoce periodos de calma y de rebrote, sobre todo al comienzo de las Primaveras Árabes y durante el último congreso que ha llevado a Xi Jinping a la cabeza del país.

Numerosos periodistas extranjeros en China han asegurado a Reporteros Sin Fronteras que tienen sus teléfonos pinchados y vigilados sus correos electrónicos. Los periodistas locales aseguran también que han empeorado sus condiciones de trabajo. Muchos desconfían de sus colegas extranjeros.

El internauta Hu Jia ha pasado tres años y medio en prisión por "incitación a la subversión". Puesto en libertad el 26 de julio de 2011, continua, no obstante, privado de todos sus derechos y sometido a arresto domiciliario. Unos meses después de su puesta en libertad, las autoridades chinas le confiscaron su ordenador para recuperar sus contactos y datos sensibles.

La vigilancia a los monjes tibetanos es algo frecuente. Las autoridades practican auténticas redadas en los monasterios. El 1 de septiembre, 60 vehículos de las fuerzas armadas de seguridad china llegaron al monasterio de Zilkar, confiscando ordenadores, DVDs, documentos y fotos de las celdas de los monjes.

La noche del 5 de noviembre de 2012, días antes del Congreso del Partido Comunista Chino, el abogado y bolguero Shu Xiangxin, fue detenido en la provincia oriental de Shandong.

El 9 de noviembre de 2012, el bloguero Cheng Zuo Liang fue llevado a la comisaría de Ningbo para ser interrogado por un asunto relacionado con la construcción de una fábrica de productos químicos contaminantes. Durante su detención la policía le recordó que tenía prohibido comunicarse con Hu Jia durante el Congreso. La policía le mostró también detalles de conversaciones telefónicas e intercambio de mensajes entre los dos, lo que confirma la vigilancia a la que está sometido Hu Jia.

En abril de 2012, el artista y militante de derechos humanos, Ai Wei Wei, se mofó del sistema de vigilancia chino, colocando cuatro web-

CHINA

cams en su despacho y en su habitación que le filmaron durante 24 horas. El sitio de "auto-vigilancia" de Ai Wei Wei fue bloqueado a las pocas horas.

Posibles soluciones técnicas

Los sitios como GitHub que combinan un servicio indispensable, desde el punto de vista económico, con funciones sociales, son todo un desafio para las autoirdaes chinas. No pueden bloquearlos o vigilarlos sin penalizar a la economía de un país entero. Por lo tanto, este tipo de servicios son un verdadero dolor de cabeza para los vigilantes de la web china y constituyen una puerta de escape para los internautas chinos.

Otros servicios, como los servidores que albergan el código fuente de aplicaciones Linux, presentan las mismas características que GitHub y son un medio ideal, aunque difícilmente accesible a los no informáticos, para pasar a través de la Gran Muralla Electrónica.

Después de la puesta a punto de la Gran Muralla Electrónica de China, los proveedores VPN han evolucionado sus tecnologías. Hasta hoy, el VPN gratuito FreeGate todavía funciona. De los VPN de pago, Astrill todavía consigue evadir la censura.

Pero el año 2012 ha demostrado que las autoridades chinas también reaccionan y hacen evolucionar su Gran Muralla Electrónica, con ocasión de acontecimientos puntuales de gran envergadura, tales como el escándalo Bo Xilai o el XVIII Congreso del Partido Comunista Chino. Los técnicos del Estado y los hackers o las empresas que ofrecen soluciones de cifrado y de evasión de la censura, juegan al gato y al ratón constantemente. "Para continuar siendo eficaces es necesario ir un paso por delante" declara un ingeniero de FreeGate. La mayor dificultad en este juego es conseguir proporcionar a los periodistas y a los interneutas las últimas versiones de los softwares.

IRÁN

Más de 150 proveedores de acceso o empresas de servicios de Internet se reparten el mercado iraní. Desde 2009 muchos de esos servicios han sido privatizados, pero no se han independizado totalmente del régimen. Los más importantes están afiliados al poder y todos los proveedores de acceso a Internet rinden cuentas al Gobierno. Entre los más importantes están DCI, propiedad de los Guardias de la Revolución, Novinnet, Shatel, Asretelecom, Pardis, Persian-Net, Tehrandat, Neda, Askiran y Tavana.

Realidad y fantasmas de la red iraní

Irán está conectado a Internet desde mediados de los años 90. Por razones económicas y políticas, las autoridades han desarrollado infraestructuras hasta el punto de convertir a Irán en el país de la región con mayor número de internautas. La red está en poder del régimen de los "mollahs", que controlan infraestructuras, tecnologías y órganos de regulación, además de imponer una legislación liberticida.

Si la gran mayoría de los iraníes se informa por la televisión, Internet tiene un papel esencial en la circulación de la información, gracias a su uso por disidentes e informadores que relatan hechos y opiniones que no están presentes en los medios tradicionales y dan testimonio de la represión en el país. Las autoridades acusan regularmente a las redes sociales de ser un instrumento a sueldo de las potencias occidentales para conspirar contra el régimen. La velocidad de conexión a Internet en Irán se ha transformado en un indicador de la situación política y del grado de vigilancia de las autoridades. La víspera de acontecimientos susceptibles de provocar protestas, la velocidad de conexión se ralentiza, para evitar el intercambio de vídeos e imágenes. La red iraní no está más politizada que otras, pero sí es la más vigilada. Todo lo que se aparta de la linea oficial es automáticamente calificado de "político" y pasa a ser filtrado o vigilado. A veces se bloquean hasta webs de moda, de música, o de cocina, que sufren la misma censura que los sitios independientes de información u oposición.

"Internet halal"

El proyecto de crear una Internet propia en Irán, que responda a los valores de la revolución, ha empezado a tomar forma. En septiembre de 2012, el gobierno de Ahmadinejad

IRÁN

aceleró su puesta en marcha, justificándola en los ataques informáticos recibidos en sus instalaciones nucleares. El Lider Supremo, Ali Jameni, apoyó la iniciativa.

Al término de la construcción de esta red paralela, dotada de una gran velocidad de conexión, pero vigilada y censurada en su integridad, todos los sitios web iraníes estarán albergados en servidores locales. Las aplicaciones y servicios, tales como correos electrónicos o redes sociales, se desarrollarán bajo el control del Gobierno. El lanzamiento inminente de esta Internet a escala nacional es inquietante. Permitirá amordazar sistemáticamente a las voces disidentes y vigilar a gran escala a los internautas iraníes.

De momento sólo están conectadas a esta red nacional las administraciones, pero se teme que los ciudadanos no tengan otra elección que sumarse a ella en el futuro. Según informaciones recogidas por Reporteros Sin Fronteras, el gobierno proyecta bajar la velocidad de conexión de la red internacional y aumentar su precio de suscripción, haciendo así la oferta de suscripción a la red nacional más atractiva, por su mayor velocidad y menor precio.

Técnicas de vigilancia

La República Islámica de Irán dispone de un amplio arsenal tecnológico y legislativo para vigilar su red. En irán son legales el filtrado, la intervención directa a los proveedores, y el espionaje a los correos electrónicos, chats o VOIP.

La complejidad de la política interior del país y las inminentes elecciones añaden a la vigilancia legal un carácter opaco, imprevisible y a veces ilógico. Testigo de ello ha sido el bloqueo de webs progubernamentales o el embrollo administrativo que siguió al filtrado de Google en Irán.

"Vigilancia oficial"

La situación política es tal, que hoy en día es casi imposible definir exactamente qué contenidos están filtrados. Desde que Ahmadinejad llegó al poder se han multiplicado las autoridades, instituciones, comisiones y comités responsables de la gestión de la red, que se hacen omnipresentes sin lógica ni concierto, respondiendo a intereses políticos, a veces inciso divergentes.

IRÁN

Los proveedores de acceso a Internet tienen la obligación de identificarse ante el gobierno y las webs deben obtener una licencia de la Compañía de Telecomunicaciones de Irán (TCI). Los blogs también tienen que registrarse en el Ministerio de Cultura y Orientación Islámica (MCOI) y después, pasar la criba del grupo de trabajo de determinación de contenidos criminales y del "Consejo Supremo del Ciberespacio", dirigido por Ahmadinejad y compuesto de Ministros, Guardias de la Revolución y personas cercanas al Líder Supremo.

Para que las informaciones que circulan en internet no contraríen el espíritu y los valores de la revolución, el filtrado se efectúa a todos los niveles con listas negras, contraseñas, URLs, IPs, etc., en función de las tensiones políticas internas. Varias webs de opinión, incluidas opiniones conservadoras y próximas a la presidencia, han sido bloqueadas, como el blog de Amir Hassan Sagha, o el de Mehdi Khazali, o como el sitio de información *Shomanews*. En 2012, varios blogueros próximos a Ahmadinejad fueron perseguidos por iniciativa del fiscal del Teherán por haber denunciado a personas cercanas al Lider Supremo, Ali Jamenei. Las rivalidades en la cima del poder entre los clanes de Jameni y de Ahmadinejad hacen cada vez más víctimas en los medios conservadores.

La censura abarca igualmente a sujetos menos polémicos, como la moda, o algunos juegos en Internet, como Travian. Las palabras clave relativas a la pornografía están evidentemente fuera de los buscadores.

Los dirigentes iraníes vigilan a la vez el acceso a las webs de información albergadas en el extranjero y en Irán. Las extranjeras, tanto en inglés, como en farsi, están frecuentemente bloqueados. La *BBC* descubrió en enero que los internautas iraníes que deseaban acceder al sito bbcpersian.com eran redirigidos hacia persianbbc.ir, cuyos contenidos son más acordes con los valores de la revolución. De igual forma, las webs de *Voice of America*, *Kaleme* o *Jaras*, están inaccesibles sin herramientas de evasión de la censura.

Redes sociales en el punto de mira

El jefe de la policía iraní, Esmaeil Ahmadi Moghadam, anunció, en enero de 2013, que el Gobienro estaba desarrollando una tecnología que permitiría un mejor vigilancia sobre las re-

IRÁN

des sociales, Tiwitter y Facebook en cabeza. Un "control inteligente" que permitiría "evitar los males de las redes sociales", pero "beneficiarse de sus aplicaciones útiles". De este aforismo sibilino hay que comprender que la cuenta de Twitter del Líder Supremo estará accesible, al contrario que la de sus opositores políticos o la de periodistas occidentales. Moghadam estima que este control será más eficaz que los bloqueos puros y simples.

Aún dudando de las capacidades reales de Irán de establecer este nuevo sistema de vigilancia, el proyecto no deja de ser preocupante. Facebook y Twitter, hasta entonces bloqueadas, volvieron a estar accesibles el 20 de febrero de 2013, una noticia que, que lejos de ser positiva, responde probablemente a un nuevo intento de vigilancia de sus usuarios.

Herramientas técnicas

Entre las herramientas del poder iraní para controlar su red se encuentran técnicas de filtrado, pero también, según fuentes de Reporteros Sin Fronteras, herramientas de tipo DPI ("Deep Pcket Inspection"). Según diversas investigaciones, algunos productos chinos ayudan a Irán a vigilar a su población, especialmente los gigantes ZTE y Huawei. El DPI proporcionado por Huawei a Mobin Net, principal proveedor iraní de la red inalámbrica, permite analizar contenidos de los correos electrónicos, buscar los históricos de navegación o bloquear el acceso a páginas web. Los productos de la firma ZTE, vendidos a la Telecommunication Compay of Iran, ofrecen los mismos servicios, así como herramientas de vigilancia para la red móvil.

Otras herramientas de espionaje y de análisis de datos provienen de empresas europeas. Se han encontrado productos de Ericsson o Nokia Siemens Network (después Trovicor). Estas empresas vendieron, en 2009, a Mobile Communication Company of Iran y a Irancell -las dos más importantes empresas de telefonía móvil en el país- productos que permitían interceptar SMSs o localizar a sus usuarios. Estos productos fueron utilizados para identificar a los ciudadanos iraníes tras las protestas populares posteriores a las elecciones presidenciales de 2009.

Lo más sorprendente es que se ha detectado material de vigilancia israelí. Las herramientas de Netenforcer fueron proporcionadas por Is-

IRÁN

rael a Dinamarca antes de ser revendidas en Irán. De la misma forma, también se ha encontrado material estadounidense, a través de la empresa china ZTE. Además de todas estas herramientas de vigilancia, los agentes iraníes utilizan también ataques "Man in the Middle", a fin de impedir a los internautas utilizar las técnicas de evasión de la censura, como Tor, proxis o VPNs.

Poderoso aparato institucional

El Estado dirige o controla casi todas las instituciones de regulación, gestión y legislación relativas a las telecomunicaciones en el país. La creación del Consejo Supremo del Ciberespacio, en marzo de 2012, demuestra que el poder centraliza sus competencias en materia de vigilancia de Internet. El Líder Supremo ha nombrado a Ahmadinejad a la cabeza del Consejo, que tiene autoridad sobre los proveedores de acceso a Internet. Según su secretario general, Mehdi Akhavan Behabadi, le corresponde tomar las mayores decisiones y coordinar las instituciones relativas a Internet.

Cuando se dio la privatización el sector, en 2009, los Guardias de la Revolución adquirieron la Telecommunication Company of Iran, propietaria del principal proveedor de acceso a Internet. Los mismos Guardias de la Revolución dirgen además el Centro de Vigilancia de Delitos Organizados y su web oficial, Gerdab. La web ha participado activamente en la búsqueda de internautas, incitando a que se les denuncie. Los Guardias de la Revolución controlan igualmente el Grupo de trabajo de determinación de contenidos criminales y están en el origen de un gran número de censuras en Internet y de detenciones de informadores.

Los Ministerios de Cultura y Orientación Islámica, de Información, y de Tecnología de la Información de la Comunicación, también tienen su parte en el control de Internet, aunque sus decisiones no escapan a los conflictos internos. Recientemente el Ministerio de Cultura y Orientación Islámica, próximo a Ahmadinejad pidió a los operadores de telefonía móvil vigilar los mensajes de texto ante las próximas elecciones. Sin embargo, la Autoridad de Regulación de las Comunicaciones matizó esta actuación, anunciando que sólo se bloquearían los mensajes comerciales. Ahmadinejad intenta actualmente situar a la cabeza del Ministerio de las Tecnologías de la Información y de

IRÁN

la Comunicación a uno de sus lugartenientes, Mohamed Hassan Nami, doctorado en Estrategia de Estado en la universidad de Pyongyang. No cabe esperar que un militar formado en Corea del Norte venga a suavizar la legislación en materia de nuevas tecnologías de la comunicación.

Además de estas entidades legisladoras existe un "ciber ejército" (FETA), y el decreto de enero de 2012, sobre las nuevas regulaciones para los cibecafés, contemplaba que os clientes presentasen su identidad y aceptasen ser filmados por cámaras de vigilancia. Los gerentes de los establecimientos tenían la obligación de conservar los registros de video, los datos completos de los usuarios y la lista de sitios visitados durante seis meses.

Legislación cada vez más liberticida

En 1979, la Constitución iraní inscribía en mármol la libertad de expresión y proscribía el uso de la vigilancia no prevista por la ley: "La inspección e interceptación de correos, la divulgación o el registro de conversaciones telefónicas, o la divulgación de comunicaciones telegráficas, la censura, la escucha y toda forma de vigilancia queda prohibida, a menos de que lo indique el Derecho", reza el artículo 25 de la Constitución. De la misma forma, el artículo 24 estipula que "las publicaciones y la prensa gozan de libertad de expresión, salvo que ataquen los principios del Islam y de la moral pública".

Sin embargo las excepciones previstas por estos dos artículos han sido ampliamente explotadas por las autoridades. La Ley de Prensa de 1986, reformada en 2000 y en 2009 para abarcar a las publicaciones en Internet, permite al poder verificar que los informadores "no atacan a la República Islámica, no ofenden al Líder Supremo y no difunden informaciones falsas". Las publicaciones en Internet están obligadas además a tener una licencia.

Dos semanas después de la reelección de Ahmadinejad, la República Islámica dio un nuevo paso para reforzar la censura en Internet, firmando la "Computer Crime Law" (CCL), en 2009. Una ley que permite la creación del Grupo de trabajo de determinación de contenidos criminales, que decide, desde entonces, lo que está o no conforme con las a leyes de la República Islámica. La CCL obliga a todos los

IRÁN

proveedores de acceso a Internet a registrar todos los datos intercambiados por sus usuarios durante seis meses, so pena de severas sanciones. Los internautas que publiquen contenido ilegales o que se sirvan de herramientas de evasión de la censura para acceder a lo contenidos bloqueados se arriesgan a graves penas de prisión. Pero el Grupo de trabajo de determinación de contenidos criminales no termina de determinar, no obstante, el carácter ilegal o no de ciertas herramientas de evasión de la censura, como las VPNs, también producidas y distribuidas por Irán, con el nombre de VPN Halal.

Violaciones a la libertad de información

Las combinación de estos arsenales tecnológicos, de un fuerte aparato legislativo, y de un contexto político interno dividido, conforman un cóctel explosivo cuya primera víctima es el pueblo iraní, que ve destrozada su libertad de información. El inicio de año 2013 ha quedado marcado por una ola de detenciones preventivas, ante la proximidad de las elecciones de junio de 2013. El régimen trata de evitar una ola de protestas (recogidas por los medios de comunicación y por Intenret) similares a las de junio de 2009.

El 27 de enero de 2013, el llamado "Domingo Negro", el régimen organizó distintas redadas en las sedes de cinco medios de comunicación de Teherán (*Etemad*, *Arman*, *Shargh*, *Bahar* y *Aseman*). Se detuvo a 15 periodistas y se anunció que muchos otros serían convocados ante los tribunales. Estos periodistas están acusados de "colaborar con medios occidentales y contrarrevolucionarios con sede en el extranjeros". 20 días después otros diez periodistas, internautas, activas políticos y miembros de la sociedad civil fueron convocados o detenidos. Durante los interrogatorios fueron amenazados y se les pidió no tener ninguna actividad durante las elecciones presidenciales de junio de 2013. Se les pidió también que revelasen la identidad de sus contactos de Facebook y Twitter y los motivos por los que contactaban con ellos.

El 18 de febrero, Ahmad Bakshaysh, miembro de la Comisión de la Seguridad Nacional del Parlamento, declaró al periódico *Roozonline* que el responsable de los asuntos culturales

IRÁN

del Ministerio de Información le había dicho que "estas detenciones son preventivas, tienen por finalidad impedir la actividad de una red en el interior y en el exterior del país, ante las elecciones presidenciales de junio (...) esta red anima a sus periodistas a entrevistar a los diferentes responsables del régimen para mostrar sus divergencias (...) al ser puestos en libertad, muchos de ellos han comprendido su error y están dispuestos a testificar en ese sentido". Ahmad Bakshaysh concluye: "Pienso que se refería a confesiones televisadas". Además de la vigilancia confesa a estos periodistas y de las intimidaciones a las que se les ha sometido, "los inspectores ejercen presiones psicológicas en los interrogatorios para que los periodistas confiesen actividades de espionaje", cuenta Reza Tajik, periodista iraní refugiado en Francia. "Estas confesiones son filmadas y difundidas por la televisión".

Estas redadas caracterizan la segunda legislatura de Ahmadinejad, marcada por la vigilancia, la censura y la detención de numerosos periodistas o bloqueros. Reporteros Sin fronteras recuerda la muerte del bloguero Sattar Beheshti, encarcelado el 31 de octubre de 2012, en circunstancias todavía desconocidas. Las informaciones que se manejan actualmente llevan a la conclusión de que sucumbió a las palizas propinadas por sus carceleros durante los interrogatorios. No se ha iniciado ninguna investigación independiente sobre su muerte, y los responsables de ella siguen impunes.

El régimen intenta infiltrarse en las redes de periodistas, tanto en el interior, como en el exterior del país. Detenido en 2010, el periodista Saeid Pourheydar, relata haber padecido malos tratos durante su interrogatorio. Los agentes le mostraron las transcripciones de sus conversaciones telefónicas, correos electrónicos y SMSs. Los prisioneros que encontró relataban hechos similares, lo que demuestra el nivel de vigilancia de los periodistas iraníes.

Los periodistas exiliados o que informan desde el extranjero (especialmente los que colaboran con *Radio Free Europe* y la *BBC*) reciben regularmente mails con software maligno, y los periodistas extranjeros autorizados a entrar en territorio iraní son vigilados de cerca, así como sus actividades en Internet. Si se conectan a las redes iraníes sus datos son inmediatamente espiados si no utilizan herramientas de seguridad y anonimato en sus comunicaciones.

IRÁN

Posibles soluciones técnicas

VPNs

Para esquivar el bloqueo y la censura de contenidos en Irán, los ciudadanos pueden utilizar las tecnologías de las redes privadas virtuales, VPNs. El Estado iraní vende este tipo de tecnologías, para aprovechar un mercado floreciente en Irán y para impedir que sus ciudadanos no lo compren en el exterior. A pesar de lo contemplado en la "Computer Crime Law", la utilización de VPNs en Irán es legal, sólo están prohibidas las extranjeras (aunque sean las que hay que utilizar).

Controlando el servidor, como lo hacen las autoridades iraníes en el caso de sus propias VPNs, se tiene todo el acceso necesario para observar y analizar el tráfico.

El Estado iraní no provee inocentemente tecnologías para esquivar su propia censura. El proveedor de la VPN tiene la posibilidad de observar y analizar todo el tráfico que pasa por ella. Aunque el tráfico esté cifrado entre el usuario, su ordenador y el servidor, no lo está entre el servidor e Internet.

Tor

Tor es una herramienta para conseguir el anonimato que protege los datos privados de sus usuarios cuando navegan por Internet. En Irán, Tor se utiliza para paliar a las VPNs cuando éstas están bloqueadas. Su utilización, sin embargo, reduce considerablemente la velocidad de navegación. Los internautas prefieren utilizar las VPNs y consideran a Tor una solución secundaria. Su única utilización va a desaparecer porque el Estado iraní tiene la posibilidad de demandar a los proveedores de acceso que identifiquen su tráfico Tor, fácilmente reconocible, y por tanto conocer su proveniencia.

Existe, sin embargo, una posibilidad para los ciudadanos de camuflar el tráfico Tor: Obfsproxy. Según sus desarrolladores, los proveedores de acceso a Internet no pueden detectar el tráfico Tor si va acompañado de Obfproxy.

Consejos

Los medios de vigilancia del régimen iraní evolucionan constantemente. Estos consejos deben tomarse con precaución, porque si hoy en día son válidos, pueden no serlo mañana. Lo

IRÁN

esencial es conocer bien y evaluar constantemente el contexto y las amenazas a las que se está expuesto.

• No utilizar las VPNs nacionales. Utilizar una VPN controlada por las autoridades iraníes equivale a lanzarse a la boca del lobo.

• El régimen no tiene hoy en día los medios necesarios para vigilar a millones de ciudadanos, algunas precauciones de base, como actualizaciones regulares, utilización de antivirus, de VPNs, o la utilización sistemática del protocolo https, permiten librarse de una gran parte del riesgo.

• Una buena "higiene electrónica": no pinchar en links enviados por destinatarios desconocidos, no cargar software de desconocida procedencia, no aceptar solicitudes de contactos desconocidos en las redes sociales o identificar al remitente de un correo electrónico antes de abrir los archivos adjuntos, permite evitar la infección de los ordenadores.

• El hecho de que algunos sitios, bloqueados en Internet desde hace tiempo, tales como Facebook, Youtube o Twitter, vuelvan a estar accesibles, suele responder a menudo a un intento de las autoridades de recuperar los nombres de sus usuarios y contraseñas mediante ataques "Man in the Middle". La utilización de una VPN no permite solamente esquivar la censura, sino también, y sobre todo, evadir los medios de vigilancia de una red, gracias al cifrado de las comunicaciones intercambiadas entre el servidor y el usuario.

SIRIA

Siria, ya cualifica como "Enemigo de Internte", por Reporteros Sin Fronteras, ha ido reforzando la censura y la vigilancia en Internet a medida que se ha ido acentuando el conflicto. Desde el inicio de la sublevación popular, el 15 de marzo de 2011, el régimen ha utilizado todos los medios necesarios para tratar de impedir la difusión de imágenes e información sobre la represión. Gracias a una arquitectura centralizada, el gobierno sirio tiene la capacidad de aislar al país del resto del mundo, como lo hizo el 29 de noviembre de 2012.

Vigilancia en la red

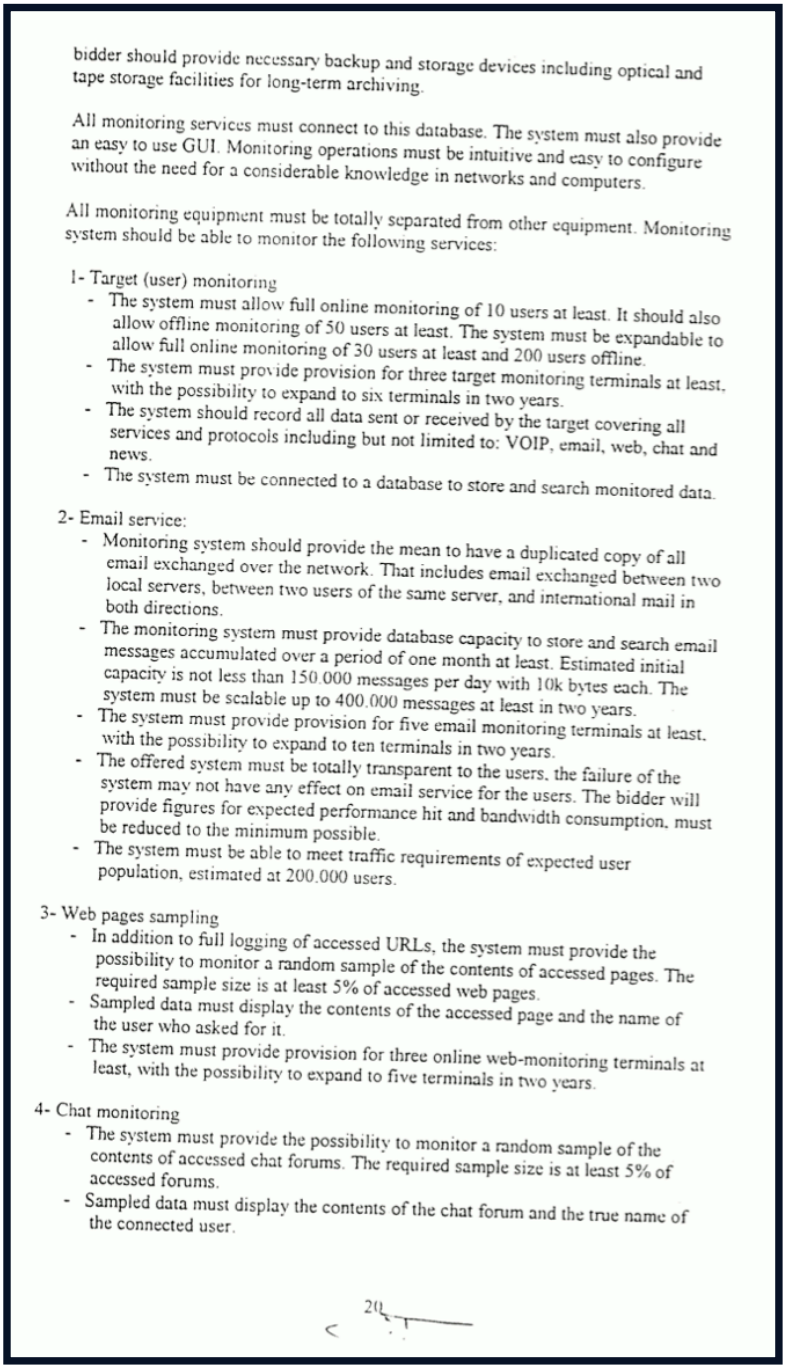
La red siria de Internet está controlada por dos entidades: La Syrian Computer Society (SCS) y la Syrian Telecommunications Stablishment (STE). La primera, fundada por Bachar Al-Assad, aporta una infraestructura 3G a todo el territorio sirio.

Situada bajo la tutela del Ministerio de las Telecomunicaciones y de las Tecnologías, la segunda, la STE, controla la mayoría de las conexiones fijas. Pone su cableado a disposición de los otros operadores, por ADSL o por línea fija de módem 56kb. Gestiona también todos los puntos de conexión del país con el sistema mundial de Internet. Cuando las autoridades ordenan el bloqueo de una palabra clave, de una URL, o de una web, la STE es la que transmite las instrucciones a los operadores.

Reporteros Sin Fronteras ha encontrado un documento inédito, una oferta publicada en 1999 por la STE para la puesta en marcha de la red nacional de Internet en Siria. Leyendo este documento aparece claramente que la red de Intenet siria está concebida en origen para integrar herramientas de filtrado y vigilancia de contenidos.

La descripción general del proyecto precisa que la STE será la única estructura que asegure la conexión con Internet. Este documento contempla que el futuro proveedor implante mecanismos de filtrado y vigilancia de contenidos de Interntet en el corazón de la red. El capítulo "Monitoring System", detalla los mecanismos de vigilancia que la STE pondría en marcha, donde la totalidad de los contenidos de los buscadores deberían estar almacenados al menos durante un mes.

SIRIA



bidder should provide necessary backup and storage devices including optical and tape storage facilities for long-term archiving.

All monitoring services must connect to this database. The system must also provide an easy to use GUI. Monitoring operations must be intuitive and easy to configure without the need for a considerable knowledge in networks and computers.

All monitoring equipment must be totally separated from other equipment. Monitoring system should be able to monitor the following services:

1- Target (user) monitoring
- The system must allow full online monitoring of 10 users at least. It should also allow offline monitoring of 50 users at least. The system must be expandable to allow full online monitoring of 30 users at least and 200 users offline.
- The system must provide provision for three target monitoring terminals at least, with the possibility to expand to six terminals in two years.
- The system should record all data sent or received by the target covering all services and protocols including but not limited to: VOIP, email, web, chat and news.
- The system must be connected to a database to store and search monitored data.

2- Email service:
- Monitoring system should provide the mean to have a duplicated copy of all email exchanged over the network. That includes email exchanged between two local servers, between two users of the same server, and international mail in both directions.
- The monitoring system must provide database capacity to store and search email messages accumulated over a period of one month at least. Estimated initial capacity is not less than 150.000 messages per day with 10k bytes each. The system must be scalable up to 400.000 messages at least in two years.
- The system must provide provision for five email monitoring terminals at least, with the possibility to expand to ten terminals in two years.
- The offered system must be totally transparent to the users, the failure of the system may not have any effect on email service for the users. The bidder will provide figures for expected performance hit and bandwidth consumption, must be reduced to the minimum possible.
- The system must be able to meet traffic requirements of expected user population, estimated at 200.000 users.

3- Web pages sampling
- In addition to full logging of accessed URLs, the system must provide the possibility to monitor a random sample of the contents of accessed pages. The required sample size is at least 5% of accessed web pages.
- Sampled data must display the contents of the accessed page and the name of the user who asked for it.
- The system must provide provision for three online web-monitoring terminals at least, with the possibility to expand to five terminals in two years.

4- Chat monitoring
- The system must provide the possibility to monitor a random sample of the contents of accessed chat forums. The required sample size is at least 5% of accessed forums.
- Sampled data must display the contents of the chat forum and the true name of the connected user.

20

En la misma sección figura el conjunto de actividades a vigilar:

• El sistema debe poder registrar las actividades en Internet y fuera de la red VOIP, chat, surf y email, de 60 individuos localizados.

• Debe proporcionar una copia del conjunto de correos electrónicos intercambiados en Siria.

• Debe registrar todas las URLs de las páginas web visitadas.

• Y debe poder vigilar de manera aleatoria el contenido de mensajes de fórums, que a su vez deben estar asociados al verdadero nombre de sus usuarios.

• Los Grupos de Noticias, poco utilizados hoy en día, pero muy corrientes en 1999, estaban también dentro del perímetro de vigilancia del régimen.

Sobre las conexiones cifradas el documento contempla también la descripción en detalle de las posibilidades de interceptación de y bloqueo de todo dato cifrado.

Si es imposible saber si el sistema utilizado en Siria desde el principio del año 2000 responde punto por punto al documento anteriormente citado, en todo caso dicho documento demuestra una voluntad feroz de las autoridades sirias de vigilar Internet.

SIRIA

Perfeccionamiento de los medios de filtrado y vigilancia

En 2011 las autoridades añadieron nuevas tecnologías a su dispositivo de vigilancia. La web Reflets.info, en colaboración con el grupo de activistas Telecomix y el portal tunecino Fhimt.com, revelaron la presencia de servidores (proxy) Blue Coat en Siria, y publicaron las pruebas de ello en sus páginas web.

En un primer momento Blue Coat negó haber vendió proxys al gobierno sirio. Pero, después de la publicación de las pruebas, admitió la presencia de al menos 13 de sus servidores en Siria, al parecer vendidos por una sociedad capacitada para vender e instalar productos Bloe Coat desde Dubai. En diciembre de 2011, la empresa Blue Coat declaró finalmente no distribuir ni soportes ni actualizaciones para los servidores instalados en Siria y no disponer de medios para desactivar sus servidores a distancia. Según pruebas llevadas a cabo en julio de 2012, por el Citizen Lab, los servidores Blue Coat sirios no se comunican con la casa madre, lo que acredita la versión de la empresa.

Ataques "Man in the Middle"

En febrero de 2011, coincidiendo con el comienzo de la Primavera Árabe, el gobierno sirio hizo accesible Youtube, Facebook y Twitter, que, habiendo estado bloqueados desde hacía años, permitieron movilizarse a los tunecinos y egipcios.

En mayo de 2011, la ONG Electronic Frontier Foundation, informó de un primer ataque "Man in the Middle" contra los usuarios sirios que se conectaban en la versión segura de Facebook.

Los internautas que se conectaban a Facebook vieron aparecer en su navegador una alerta de seguridad que les indicaba que el certificado (el documento que identifica la identidad de un sitio) no era válido. Los que se conectaron a su cuenta sin hacer caso a esta advertencia, permitieron a los atacantes hacerse con su nombre de usuario y contraseña.
En julio de 2011, la sociedad editora del certificado, Diginotar, detecta una intrusión en su red.

Entre julio y agosto de 2011, el grupo hackers activistas Telecomix lanza la operación OPSyria

SIRIA

y recupera más de 54Go de informaciones sobre el funcionamiento de los servidores Blue Coat.

En agosto de 2011, las versiones https de Facebook y de Yahoo, fueron bloqueadas en Siria y automáticamente redirigidas hacia versiones no seguras http (forzando así a los internautas a dar sus contraseñas). En este tipo de maniobras el único índice que permite verificar que las contraseñas están cifradas cuando se envían en Internet es la letra "s" en url, y el símbolo de una cadena al lado. Los internautas menos atentos caen en la trampa.

A finales de agosto de 2011, Google detecta la utilización de un certificado DigiNotar fraudulento en Irán.

Los ficheros recuperdos por la operación OP-Syria permiten suponer que las autoridades sirias utilizan ataques "Man in the Middle" muy evolucionados. Los periodos de conexión de los servidores Blue Coat no deberían normalmente registrar informaciones cuando un internuta accede a un sitio seguro (https), sin embargo, cuando se accede a los sitios más consultados en Siria, estos periodos de conexión revelan que los servidores Blue Coat han registrado un número anormalmente elevado de informaciones no accesibles en tiempo normal ya que estám cifradas. Esto está probablemente unido al robo de certificados de la sociedad DigiNotar.

Tiro al blanco

Las armas infromáticas del régimen sirio no se limitan al mero análisis del tráfico en Internet. Bloomberg y Citizen Lab han informado de los métodos de vigilancia apurados de las autoridades sirias.

Un caso emblemático: Karim Taymour

En su artúculo "Hackers in Damascus", el periodista de Bloomberg, Stefan Faris, detalla el caso de Karim Taymour, un activista sirio detenido y torturado por el régimen. El 26 de diciembre de 2011, mientras se dirigía a una cita con uno de sus contactos, Katim Taymour fue detenido por las fuerzas de policía sirias. La cita la había concertado esa misma mañana por Skype, pero las autoridades estaban al corriente. Karim pasó 71 días detenido. Durante su interrogatorio se negó a desvelar sus acti-

SIRIA

vidades y contactos, pero le presentaron más de 1000 páginas detallando conversaciones y ficheros intercambiados por Skype. A pesar de la resistencia que opuso a sus carceleros, lo cierto que es éstos ya tenían suficiente información por su ordenador.

En enero de 2012, un mes después de la puesta en libertad de Karim Taymour, Morgan Marquis Boire, un experto en seguridad de Google, recuperó el ordenador de un miembro de una ONG en Siria que desconfiaba que su material estaba infectado. Tras un exhaustivo análisis, Marquis descubrió que el ordenador había sido intervenido una primera vez, el 26 de diciembre, horas después de la detención de Karim. El software espía fue transmitido a este miembro de la ONG por un mensaje de Skype enviado por Karim Taymour. El software estaba camuflado en un documento que Karim había terminado la víspera de su detención.

"Phishing" e ingenieria social

El caso de Karim Taymour es representativo de los métodos utilizados por el régimen sirio para vigilar y detener a los internautas. Es esquema de ataque es siempre el mismo: durante una conversación, un contacto propone a su interlocutor que cargue un video, un documento o una imagen. El link propuesto es un software espía que, en cuanto se pincha, se instala en el ordenador. Las cuentas Skype utilizadas son las de ciudadanos detenidos o cuyo ordenador ha sido infectado y se crean cuentas especiales para cazar a los internautas.

La campaña de infección "Blackshade", llevada a cabo a partir de junio de 2012, en Siria, fue descubierta gracias a un mensaje enviado desde una cuenta de Skype a un miembro de la oposición siria.
La traducción del mensaje decía: "Hay alguien que te detesta y que no deja de hablar de ti. Tengo un registro de la conversación, deberías desconfiar de esta persona porque te conoce personalmente. He aquí el registro de la conversación". Cuando el internauta pincha el "malware" se instala sobre el ordenador de la víctima.
El régimen utiliza también ataques de tipo "phishing". Un tipo de ataque que consiste en colocar una copia de un sitio conocido, como Youtube o Facebook, que pide al internauta aportar informaciones personales por motivos aparentemente creíbles. Se le propone poner

SIRIA

al día su perfil o aceptar una nueva política de confidencialidad.

En marzo, una falsa página de Youtube, que supuestamente tenía vídeos de la oposición, pedía a los internautas entregar su contraseña para añadir comentarios. Además, permitía instalar un software espía solicitando a los visitantes cargar una puesta apunto del Adobe Flash.

En abril de 2012, el EFF registró al menos cinco intentos de "phishing" hacia usuarios de Facebook. Uno de ellos consistía en mensajes publicados en las cuentas de Facebook de líderes de la oposición siria, entre ellos Burhan Ghalioun. Pinchar sobre los links dejados en estas páginas enviaba hacia una falsa página de Facebook que proponía instalar una aplicación, FacebookWebBrowser.exe, supuestamente destinada a la mejora de la seguridad de las cuentas de Facebook. FacebookWebBrowser.exe es un software espía que permite recuperar todos los caracteres marcados en un teclado y robar los nombres de usuario y contraseñas de cuentas, email, Youybe, Facebook y Skype.

En agosto de 2012, el EFF identificó una nueva ola de difusión del software espía bajo la forma de un programa llamado Antihacker, que supuestamente protegía al ordenador donde se instalaba. Antihacker no es software espía en sí mismo, sino que, una vez instalado, instala en el ordenador de la víctima una versión de DarkComet, un software capaz de registrar imágenes de la webcam del ordenador, desactivar las notificaciones de ciertos antivirus, registrar los golpes de teclado y recuperar las contraseñas.

La mayor parte de los ataques han sido realizados con al ayuda de los mismos softwares espías: DarkComet o BlackShade. Una vez instalados sobre un ordenador o un teléfono, permiten tener acceso a la webcam, contraseñas de las cuentas, correos electrónicos, Youtube, Facebook, conversaciones de Skype o golpes de teclado. Las informaciones recuperadas son enviadas hacia servidores cuya dirección está situada en Siria, lo que hace suponer que estos ataques provienen del mismo "ciber ejército" sirio.

Este grupo progubernamental estaría igualmente en el origen de la falsa página Youtube

SIRIA

que ha servido para el ataque "phishing" descrito anteriormente. En julio de 2012, difundió 11.000 nombres y contraseñas de "apoyantes de la ONU". Según algunos expertos, este grupo paramilitar trabaja en estrecha colaboración con los servicios secretos sirios.

Posibles soluciones técnicas

La primera medida a tomar en Siria es proteger los ordenadores de softwares malignos. Para hacerlo hay que respetar algunos consejos de base:

• No instalar ningún software recibido por correo electrónico.

• No instalar ningún software, excepto aquellos de un sitio "https", donde el riesgo de usurpación de identidad está muy reducido

• No instalar ningún software que provenga de una fuente que no sea familiar, incluso si la instalación está recomendada por una ventana emergente.

• Hacer sistemáticamente actualizaciones del sistema y de los softwares instalados.

• No utilizar Internet explorer para navegar en Internet. Siendo este navegador uno de los más utilizados, es también el más atacado. Es preferible el uso de Firefox o Chrome.

• Erradicar softwares malignos: Siendo DarkComet uno de los peores hay softwares que permiten destruirle. El EFF ha publicado una guía que permite suprimir softwares espías muy utilizados: Xterm Rat.

• Proteger la navegación en Internet y prevenir Mitim: Existen soluciones que permiten protegerse contra los ataques Mitim. La más simple es ignorar las advertencias de seguridad del navegador de Internet cuando se conecta a un sitio "https". Existen extensiones para los navegadores Chrome y Firefox que permiten detectar los ataques Mitim como "https everuwhere".
Esta extensión comprueba si existe una versión https (cifrada) para cada sitio y en su caso le redirige hacia ella. Pueden darse entonces varios escenarios:
-Si hay un intento de "phishing", los que hayan instalado esta extensión serán redirigidos hacia la versión https del sitio.

SIRIA

-Si el ataque es básico, el internauta es redirigido hacia la verdadera versión https de Facebook.
-Si el ataque es elaborado, los internautas reciben una alerta de seguridad que les indica que el sitio en cuestión no es el que dice ser.
-Si el ataque es muy elaborado, y los atacantes han conseguido comprometer el certificado de Facebook, entonces es necesario verificar manualmente la autenticidad del certificado.
"https everuwhere" es útil en el uso cotidiano. Cada vez que se envían datos en Internet utilizando un formulario es indispensable utilizar protocolos https. Si no se hace, todos sus datos se transmiten sin cifrar con el riesgo que ellos comporta.

• Certificate Patrol: Esta extensión verifica los certificados. Advierte al usuario si detecta un cambio de certificado y es indispensable contra ataques "Man in the Middle".

VPN y Tor

La utilización de VPNs y de Tor, si es posible, es un medio eficaz de prevenir ataques "phishing" o "mitin". Utilizando Tor o VPNs el internauta no navega sobre la res Siria, sino sobre su punto de partida en Suecia o en Estados Unidos, librándose así de los ataques llevados a cabo en la red siria. El uso de VPNs y Tor es un buen medios de librarse de la vigilancia de la red, ya que ocultan la dirección IP de los usuarios. Finalmente, la solución VPN tiene una ventaja suplementaria, puesto que el tráfico enviado, cuando se utiliza, está cifrado, contrariamente a la red Tor, que lo único que hace es "anonimizar" al internauta.

VIETNAM

El gobierno vietnamita, al igual que el de muchos países autoritarios, se debate entre el deseo de un desarrollo económico impulsado por las nuevas tecnologías y el miedo a la inestabilidad política que pueden causar. Vietnam, con acceso a Internet desde finales de los 90, cuenta con las infraestructuras e instituciones para Internet desde mediados de la década de 2000. La creación del Comité Directivo Nacional para las Nuevas Tecnologías de la Información y la Comunicación (TIC) y el lanzamiento del Plan Nacional para el Desarrollo de las TIC, en 2005, llevó al desarrollo de Internet en el país. Una expansión de la red que ha coincidido con la aparición de blogs y cibercafés, pero también de herramientas de seguimiento y control de los internautas.

A día de hoy, el Partido Comunista de Vietnam (PCV) amplía sus miras en el campo de las telecomunicaciones, un mercado muy dinámico en Vietnam. Cada vez hay más usuarios de la red y, en Hanoi y Ho Chi Minh City, el 95% de los habitantes de 15 a 22 años tienen acceso a Internet. La juventud de la población vietnamita y la urbanización del país auguran una explosión del número usuarios de Internet en los próximos años.

Calidad y velocidad de Internet

Pero, a pesar de todos estos factores, Internet "no despega" en Vietnam. Su calidad y velocidad son inferiores a las de otros países asiáticos y, según el informe Akamai 2012, Vietnam tuvo una velocidad de conexión de 1,25 Mbps en el tercer trimestre de 2012, por detrás de Tailandia y Malasia, y muy por debajo de la media internacional, de 2 de 3 Mbps. La velocidad de conexión ha disminuido desde principios de 2012 por una simple razón: el Partido Comunista limita voluntariamente la velocidad de la re, a través de los proveedores de servicios de Internet (ISP) que controla.

Proveedores de acceso en manos del Partido Comunista

La mayor parte de los 16 proveedores de servicios de Internet está directa o indirectamente controlada por el Partido Comunista. Viet Nam Post y Telecommunications (VNPT) posee el 74% del mercado y pertenece al Estado, como Viettel (propiedad del Ejército Popular Vietnamita). FPT Telecom es una empresa privada, rinde cuentas al Gobierno y depende del ancho de banda asignado por los líderes del mercado.

VIETNAM

Hay una distinción entre los proveedores que pertenecen a particulares, empresas de acceso a Internet, y los Puntos de Intercambio de Internet (IXP) que proporcionan el ancho de banda a los ISP. Según la ley vietnamita, aunque las primeras puede pertenecer a empresas privadas, estas últimas tienen la obligación de ser statales. Un sistema que permite a las autoridades decidir qué contenidos estarán accesibles, bien por las empresas privadas que poseen, bien por los puntos de intercambio.

Dispositivo de vigilancia

Los proveedores de acceso a Internet son las primeras herramientas de control y vigilancia en Vietnam. Bloquean el acceso a sitios considerados no aptos por el régimen. Utilizan la técnica de bloqueo DNS (Domain Name Server) que elimina el acceso a un sitio por el nombre de dominio utilizado. El bloqueo del DNS afecta al sitio al completo, no sólo una página en particular, y cada proveedor tiene la posibilidad de eliminar un contenido sin coordinarse con otros actores del mercado

Por ejemplo, Facebook se censura en VNPT, mientras que los otros dos principales proveedores permiten su acceso. El centro de investigación OpenNet Initiative ha estudiado los sitios censurados en Vietnam, en 2012 y ha descubierto, entre otras webs, hay algunas de de periódicos, blogs (vietnamitas y extranjeros), páginas de oposición política, de derechos humanos, etc.

Algunos blogueros utilizan un software (proxy, VPN, Tor) para evadir la censura. Pero estas herramientas no siempre son fiables. Las autoridades tienen la capacidad de inutilizar estas soluciones mediante el bloqueo de los puertos del transporte de datos cifrados. Los blogueros controlados por el régimen sufren ataques "Man-in-the-Middle", cuyo objetivo es interceptar los datos enviados al acceder a páginas seguras (https).

Este tipo de ataque puede realizarse desde los administradores de red vietnamita, es decir, los ISP, y no es raro que se pirateen las contraseñas o que la conexión a Internet se ralentice durante los días en que los disidentes están detenidos o se enfrentan a procesos judiciales.

VIETNAM

Suscripción y datos personales bajo control

Para suscribirse a una línea fija (de teléfono e Internet), debe proporcionarse una cantidad de datos personales que incluyen la fecha de nacimiento, el número de teléfono, trabajo, empresa para la que se trabaja y comprobante de domicilio. En Vietnam la única prueba que justifica un domicilio es el "hô khâu", un documento que emite la policía y permite el control de la población. Sin el "hô khâu" no es posible alquilar un piso, encontrar un trabajo oficial o abonarse a Internet. Sólo tres países en el mundo utilizan este tipo de documento: China, Corea del Norte y Vietnam.

Teléfono móvil bajo vigilancia

Los principales proveedores de acceso a Internet son también los proveedores de la telefonía, fija o móvil. Los ingresos aproximados del mercado de la telefonía móvil en 2012 alcanzaron los 500 millones de dólares. Vietnam cuenta con 119 millones de suscriptores para 91 millones de habitantes, y tres grandes operadoras móviles, como Vittel que tiene el 90% del mercado, todas controladas por el Estado.

Según el informe de Freedom House, de julio de 2012, el 91% de los internautas encuestados accedían a internet a través de su dispositivo móvil. Pero navegar por Internet a través del móvil es menos seguro y se puede controlar más fácilmente, sobre todo cuando el Estado tiene operadores. El mismo informe acusa al gobierno de escuchar las conversaciones de los ciudadanos y de crear listas negras de internautas, calificados como "activistas" o "reaccionarios". Algunos han visto cortado su acceso a Internet o a la red telefónica.

Un arsenal jurídico liberticida

La ley de prensa de 1989 es clara sobre el papel que debe desempeñar la prensa en Vietnam. "La prensa en la República Socialista de Vietnam incluye todos los medios necesarios para la vida social, es la voz del Partido, el Gobierno y las organizaciones sociales, así como una plataforma para la expresión de la voluntad del pueblo". Esta legislación determina el espacio que debe ocupar la prensa tradicional y las publicaciones en Internet. La libertad de prensa, la libertad de expresión y el derecho a la información están recogidos en el artículo 69 de la Constitución vietnamita de 1992, pero,

VIETNAM

en la práctica, estas libertades se ven mermadas si contradicen la linea marcada por el Partido Comunista Vietnamita.

En la Ley de 1989, y el Decreto 55/2001/ND-CP, de agosto de 2001, se sentaron las bases para una red controlada por el Partido Comunista. El artículo 6 establece que la información publicada en Internet debe cumplir la Ley de Prensa; el artículo 8 del Decreto establece claramente que "los organismos competentes estatales procederán al control de la información en Internet"; su artículo 11 prohíbe el uso de Internet para oponerse a la República Socialista de Vietnam; y el decreto también establece que los puntos de intercambio de Internet (ver más arriba) no puede pueden ser de otra propiedad sino la estatal (artículo 13). En 2003, un nuevo decreto (92/2003/QD-BBCVT) prohibió "enviar o recibir material antigubernamental". El decreto también requería a los dueños de un sitio web en Internet que se registraran en el Centro Vietnamita de Información en Internet, vinculado al Ministerio de Información y Comunicación. Desde junio de 2006 (Decreto 56/2006/ND-CP), los periodistas y los blogueros están obligados a respetar la "linea revolucionaria", so pena de ser acusados de "difundir ideología reaccionaria" o de difundir "propaganda contra la República Socialista de Vietnam", un delito castigado con penas de 3 a 20 años de cárcel y multas de 2.000 dólares.

Los cibercafés son muy pululares en Vietnam, y están sujetos a estrictas regulaciones. En 2010, un Comité Popular de Hanoi obligó a los propietarios de cibercafés a instalar equipos de vigilancia aportados por el Gobierno para vigilar las actividades de los usuarios en Internet y proceder al bloqueo de algunos sitios web. Los visitantes deben proporcionar su tarjeta de identidad y los cibercafés tienen la obligación de conservar sus datos por si los quisieran controlar las autoridades. Según fuentes de Reporteros Sin Fronteras, los responsables de los cibercafés suelen hacer la vista gorda ante estas obligaciones por razones económicas y los clientes cambian de establecimiento cuando se les pide su identidad. Sin embargo, los cibercafés están obligados a conservar todo el historial de navegación de sus usuarios.

En abril de 2012, Reporteros Sin Fronteras denunció un proyecto de Decreto sobre la gestión, prestación y utilización de servicios de Internet. El Decreto venía a reemplazar uno de

VIETNAM

2008 (que a su vez reemplazó a otro del 2001) y tenía como objetivo:

• Eliminar el anonimato en Internet, quedando prohibido a los internautas ocultar sus datos o aportar datos ficticios.

• Prohibir el uso de nombres falsos en redes sociales.

• Pedir a los administradores de un sitio web que denuncien a las autoridades las actividades ilegales que en él se produzcan.

• Obligar a los blogueros a registrarse con su verdadero nombre (a menudo utilizan alias en un intento de escapar de la vigilancia).

• Exigir a las empresas extranjeras que establezcan sus centros de datos en Vietnam.

• Exigir a las empresas extranjeras que proporcionen información personal de sus usuarios (nombre, apellidos y dirección) y cooperen con las agencias gubernamentales.

Control en el corazón de las instituciones

Las decisiones sobre Internet emanan principalmente del Ministerio de Información (MIC) y del Ministerio de las Comunicaciones y Seguridad Pública (MPS).

• Ministerio de Información y Comunicación (Fuente: Libro Blanco 2011 sobre Información y Comunicación en Vietnam): El MIC dirige el principal proveedor de acceso a Internet, el Vietnam Internet Network Information Center y publica la mayoría de los decretos sobre Internet. Este ministerio trabaja con el Comité Directivo Nacional para las nuevas Tecnologías de la Información y la Comunicación, presidido directamente por el Primer Ministro.

• Ministerio de la Seguridad Pública: Este departamento gestiona más la legislación y las sanciones sobre publicaciones "reaccionarias" que los verdaderos problemas "técnicos" relacionados con la supervisión de la red. Dirige a la "ciber policía" Cong An Mang (CAM), fundada originalmente para luchar contra el delito informático, como el fraude de tarjetas de crédito, hacking, etcétera. Pero en la actualidad posee

VIETNAM

la facultad de bloquear blogs o webs incómodas y de detener a sus responsables. Según el teniente coronel Dinh Hữu Tan, jefe de la oficina de "política de seguridad interna" de Hanoi, el papel de la policía es "vigilar los contenidos de Internet, de cualquier forma, de todas las publicaciones, incluidos artículos de periódicos o comentarios de blogs". El control de Internet es oficial, pero los métodos empleados por la ciber policía siguen siendo desconocidos.

"Ciber Ejército"

A pesar de las leyes e instituciones relacionadas con la vigilancia y la censura de Internet, y de la fuerte represión a los informadores, la red vietnamita ha demostrado una vitalidad poco común. En el país florecen los blogs políticos y sociales que las autoridades intentan controlar con un "ciberejército" comprometido con la lucha contra los "antipatriotas y reaccionarios". Este "ciber ejército" no es un órgano oficial del gobierno, pero se estima que hay más de 80.000 "guardias rojos" o "espías informáticos" en el país.

En el modelo chino, esta milicia impone la propaganda del régimen y denuncia ante las autoridades las actividades de blogueros, activistas e internautas. Millares de "ciber soladados", nombrados oficialmente, tienen la misión de infiltrarse en las redes sociales y blogs de los informadores.

Violaciones de la libertad de información

El blog, un fenómeno que tiene mucho seguimiento entre los vietnamitas, es el primer objetivo de las autoridades. Huynh Ngoc Chenh (nominado premio internauta 2013) resume la situación: "Todas las comunicaciones están controladas por el Estado, las opiniones opuestas al él no se hacen públicas, la libertad de expresión es prácticamente inexistente en Vietnam, así que muchas personas utilizan los blogs para difundir sus propias opiniones. Pero estos blogs son cerrados por el gobierno, y muchos blogeros detenidos y sus familias perseguidas", El blog es sin duda un gran espacio para la expresión en Vietnam, pero también blanco de fuertes sanciones.

En septiembre de 2012, se promulgó el decreto 7169/VPCP-NC, directamente dirigido tres

VIETNAM

de los blogs más influyentes en Vietnam: Danlambao y Biendong Danglambao. Sus autores, que escribían bajo seudónimos, se enfrentan ahora a penas de prisión si se descubre su verdadera identidad. El anonimato es generalizada en la blogosfera vietnamita, pero el Partido Comunista utilizada todas las herramientas de control a su alcance para descubrir la identidad de algunos glohueros, que ahora se somenten a pesadas penas de cárcel si se descubre su identidad.

Fue el caso de Le Nguyen Sang y Huynh Nguyen Dao, en 2006. A pesar de firmar con seudónimos fueron identificados por la policía y condenado a cuatro años y medio de prisión. Tran Huynh Duy Thuc, en 2009, y Lu Van Bay, en 2011, también fueron detenidos cuando firmaban sus artículos con nombres falsos. El primero está cumpliendo 16 años en prisión, mientras que Lu Van Bay, que ha llegado a utilizar cuatro seudónimos difirentes, fue condenado a cuatro años de cárcel.

Posibles soluciones técnicas

Para proteger su anonimato, es preferible utilizar proxies VPN, que pueden evitar el bloqueo. El uso del servicio de correo anónimo, como Hushmail o riseup.net acoplado el sistema de cifrado PGP también puede ser útil.

Deben evitarse las conversaciones o teléfonos VoIP. La vigilanci en Vietnam es también física y una manera de interceptar conversaciones telefónicas o de VoIP es el uso del micrófono de largo alcance desde los alrededores de los-domicilios de los presuntos activistas. El uso de un servicio de mensajería instantánea, el chat de Google, ICQ, IRC, Yahoo, etc. junto con el software de cifrado como OTR puede frustrar este tipo de control.

AMESYS

Amesys, sociedad francesa de seguridad informática, ha vendido subproducto, el sistema Eagle, a la Libia de Gadafi. Esta tecnología fue utilizada para vigilar a periodistas y activistas de derechos humanos. La empresa ha sido llevada ante la justicia francesa por la Federation Internationale des Droits de L´Homme (FIDH), por complicidad en torturas.

La sociedad

Amesys es una sociedad francesa creada en 1979 bajo el nombre de i2e. Está especializada en tecnologías de la Información. En 2004 cambió de nombre y se transformó en Amesys.

En 2010 fue comprada por la sociedad francesa de informática Bull.

En 2011 una ONG de defensa de los derechos humanos, la FIDH, la acusó de complicidad con torturas.

En 2013 Amesys cedió su sistema Eagle a una tercera sociedad, Naxos. Eagle se desarrolla y comercializa ahora por un grupo de antiguos empleados de Amesys, bajo la dirección de Stephane Salies, antiguo director de Bull.

Expediente

El sistema Eagle permite a los agentes gubernamentales vigilar el tráfico de Internet y almacenar datos de conexión para ponerlos a disposición de la policía o de agentes de información.

Según el manual proporcionado por Amesys "la tecnología Eagle está pensada para ayudar a las autoridades a aplicar la ley, y a los organismo de información a reducir el nivel de criminalidad, protegerse de una amenaza terrorista e identificar todo potencial ataque a la seguridad de un país".

La solución Eagle está compuesta de una red de análisis, de varios sistemas de almacenamiento y de centros de vigilancia para analizar los datos. El software permite la creación de fichas individuales, una por cada objetivo. Cuando los rebeldes libios penetraron en los locales de la policía secreta de Gadafi encontraron ejemplares de este tipo de fichas. El sistema Eagle se basa en la tecnología de "Deep packet inspection" (técnica de análisis en profundidad del contenido que circula en una red), y puede analizar cualquier tipo de actividad re-

AMESYS

lacionada con una web. Según Amesys, las diferentes actividades que pueden inspeccionarse son el correo electrónico (smtp, pop, imap, y webmail), los servicios VOIP, protocolos de mensajería instantánea, las solicitudes enviadas a los buscadores, y el conjunto del tráfico web-http.

Implicaciones en Libia

Los productos Amesys se han encontrado en Libia, donde la empresa tenía un contrato con la sociedad secreta de Gadafi. Los reporteros del *Wall Street Journal* encontraron manuales de utilización del sistema Eagle, así como archivos individuales de ciudadanos libios, entre ellos el del periodista libio Khaled Mehiri. El *Wall Steet Journal* demostró que sus correos electrónicos, entre ellos algunos intercambiados con *Al Jazeera*, y sus publicaciones en Facebook, habían sido vigilados durante meses por herramientas de Amesys. En enero de 2011, mientras terminaba la Primavera Árabe en Tunez, y comenzaban a aparecer problemas en Libia, Khaled Mehiri fue convocado por agentes del régimen y sometido a presiones para disuadirle de publicar declaraciones de militantes anti-Gadafi. Tras esta detención siguió vigilado y, por miedo a la seguridad de su familia, tuvo que ocultarse durante meses hasta que terminaron los enfrentamientos en Libia.

La FIDI ha denunciado a Amesys por complicidad en torturas, en nombre de cinco ciudadanos libios, espiados por medio de Eagle. "La cámara de instrucción ha confirmado que había material para instruir el caso, a pesar de los obstáculos puestos por el fiscal de París, visiblemente reticente a permitir una instrucción imparcial e independiente en este asunto", declaró Patrick Baudouin, abogado y presidente de honor de la FIDI.

En septiembre de 2011, Amesys publicó un comunicado reaccionando a las informaciones aparecidas en varios medios de comunicación sobre sus actividades en Libia.

BLUE COAT

Sociedad estadounidense de seguridad en Internet, es conocida sobre todo por sus herramientas de vigilancia de la red, que permiten el seguimiento a periodistas, internautas, así como sus fuentes. Sus herramientas se basan en la tecnología de análisis "Deep packet inspection" , utilizada por muchísimos proveedores de acceso a Internet occidentales para regular su tráfico e impedir conexiones indeseadas.

La sociedad

Blue Coat es una sociedad especializada en tecnologías de la información situada en la Silicon Valley de California, conocida sobre todo por haber proporcionado herramientas de filtrado y censura a países como Siria o Birmania. Pero la empresa tiene también un sistema de análisis de red llamado "Inteligence Center", utilizado por empresas y Estados para vigilar el tráfico y detectar problemas técnicos. Permiter igualmente vigilar el comportamiento de internautas.

Expediente

Blue Coat propone a sus clientes la tecnología "Deep packet inspection" (DPI) y "PacketShaper" que puede ser utilizada para vigilar y censurar contenidos en internet. Con el DPI es posible analizar cada paquete IP y darle un tratamiento específico, basado en su contenido (censura a palabras clave) o su tipo (email, VOIP, protocolo BitTorrent). El DPI no sólo contraviene el principio de neutralidad de la red que defiende Reporteros Sin Fronteras, sino que se opone igualmente al principio de la protección de datos personales. Hace a los internautas identificables y, en los países donde no se respetan los derechos humanos, expone a los ciudadanos a riesgos de encarcelamientos arbitrarios, violencias y torturas.

Blue Coat describe así uno de sus productos, PacketShaper: "Es su red. Haga usted lo que quiera (...) PacketShaper analiza y reconoce el tráfico generado por centenares de aplicaciones profesionales y recreativas. Gracias a su integración a WebPulse, servicio de inteligencia web en tiempo real de Blue Coat, puede incluso controlar el tráfico de aplicaciones por categorías de contenidos web (...). PacketSha-

BLUE COAT

per facilita el control agrupado de aplicaciones y contenidos asociados".

El DPI es potencialmente peligroso para periodistas blogueros y activistas, así como para sus fuentes en la medida en que su principio se dirige contra la naturaleza privada y el anonimato de la comunicación en Internet. La sociedad Blue Coat vende sus productos tanto a agentes gubernamentales como a empresas privadas, lo que la distingue de otras sociedades de este informe.

Implicaciones en Birmania

En 2011, se encontró la presencia en Birmania de 13 dispositivos Blue Coat. Muchos internautas recibieron mensajes sospechosos sobre Internet, he aquí el contenido de uno de ellos: "Queridos clientes, el 17 de octubre de 2011, a causa de una avería del cable óptico submarino, SIA-MI-WE3, la conexión a Internet está inestable. Durante el periodo de reparación, realizado por personal cualificado, la conexión a Internet puede ralentizarse o incluso no estar disponible. Les tendremos informados y nos excusamos por las molestias causadas. Respetuosamente Yatanarpon Teleport".

Implicaciones en Siria

El colectivo Telecomix, un importante grupo de hackers, que ha ayudado a mantener una conexión a Internet en Egipto y otros países de la Primavera Árabe, mientras que los gobiernos intentaba cortar la conexión, publicó, en 2012, 54 registros de conexión. Según Telecomix, estos elementos prueban que en Siria habían sido instalados 15 servidores Blue Coat. Estos aparatos fueron descubiertos en la red de proveedores Sirian Telecommunications Establishment (STE), propiedad del Estado.

Los intentos de conexión a Youtube, Twitter y Facebook, estaban relacionados y podrían potencialmente ser objeto de una investigación. Stephan Urbach, miembro de Telecomix ha declarado que estos datos tenían, no solamente históricos de conexiones, sino también contenidos de los internautas.

El análisis de los registros de conexión sugiere que los proxies de Blue Coat fueron utilizados para interceptar y analizar tráfico codificado. Todos los pedidos que utilizaban el puerto 443 (dedicado al protocolo https) con destino a los sitios web más frecuentados en Siria, conte-

BLUE COAT

nían más información de la necesaria. Estas informaciones están normalmente protegidas por una capa de cifrado que supuestamente impide la lectura por parte de los proxy.

"No deseamos que nuestros productos sean utilizados por el gobierno sirio o por cualquier otro país sometido a embargo por Estados Unidos", declaro Steve Daheb, vicepresidente de Blue Coat, en un primer intento de explicación. Según él, Blue Coat está "entristecida por el sufrimiento del pueblo sirio y de pérdidas humanas".

En un informa del Wall Street Journal, del 29 de octubre de 2011, Blue Coat reconocía que 13 de sus aparatos, en principio enviados por un distribuidor de Dubai, con destino al Ministerio de Comunicación iraquí, fueron encontrados en Siria. La empresa declaró que estos aparatos no estaban "en condiciones de utilizar el servicio WebPulse o de hacer funcionar la base de datos WebFilter", componentes importantes del dispositivo de vigilancia. Blue Coat indicó también que los aparatos en cuestión "funcionaban de forma completamente independiente" y que no podían desactivarlos a distancia. Según una serie de tests realizados, en julio de 2012, por el Citizen Lab, los equipamientos vendidos por Blue Coat a las autoridades sirias no estarían interactuando con los servicios de "cloud" de la empresa.

Otras implicaciones

Como se explica en un informe detallado del Citizen Lab, de la Universidad de Toronto, en Egipto, Kuwait, Catar y Arabia Saudí se han utilizado también sistemas Blue Coat potencialmente con fines de censura. El Citizen Lab también ha observado que en Bahréin, China, India, Indonesia, Irak, Kenia, Kuwait, Líbano, Malasia, Nigeria, Qatar, Rusia, Arabia Saudí, Corea del Sur, Singapur, Tailandia, Turquía y Venezuela, han utilizado herramientas que pueden ser usadas para la vigilancia de la actividad de los internautas.

GAMMA

Gamma International propone software espía muy elaborado. Se han encontrado en Bahréin y en Emiratos Árabes Unidos. La tecnología "FinFisher" que vende Gamma es capaz de leer archivos encriptados, correos electrónicos y registrar llamadas VOIP. Entre los objetivos de esta vigilancia ha estado Ala´a Shehabi, periodista bahrení, que ha tenido que abandonar su país y vivie actualmente en Estados unidos.

La sociedad

Gamma International es una filial del Gamma Group, con sede en Reino Unido. Tiene oficinas en el Reino Unido, incluidos Jersey y Guernesy, en Alemania, en el sureste asiático y en Oriente Medio. Está especializada en vigilancia "online" y "offline" y da formaciones en seguridad informática.

"El grupo Gamma, creado en 1990, ofrece técnicas avanzadas de vigilancia, soluciones de control de las comunicaciones, y formación a gobernantes. Ofrece consejos a los agentes de información gubernamentales y a las fuerzas del orden".

Gamma internacional pertenece a Louthean John Alexander Nelson, hijo del fundador del grupo William Louthean Nelson, y a Martin Johannes Münch (a través de Mu Shun Gmbs), más conocido por sus iniciales MJM. Gamma Internationale tiene lazos con la compañía alemana Elaman, con la que comparte una misma dirección y número de teléfono. Gamma Internationale ha confirmado a Reporteros Sin fronteras que Elaman le presta servicios como vendedor.

Expediente

Gamma Internationale vende su material exclusivamente a gobiernos y a servicios encargados de aplicar la ley. Su producto "FinFisher" utiliza software maligno capaces de infectar ordenadores, teléfonos móviles y servidores, y está considerado como uno de los más avanzados hoy en día. Un ordenador o un smartphone pueden ser infectados a distancia por un caballo de Troya, guiado por agentes gubernamentales mediante servidores de control. Un ordenador puede ser contaminado por falsas actualizaciones y notificaciones de software o por correos electrónnicos infectados. "FinFisher" ofrece también una tecnología que permite infectar todo un cibercafé para vigilar a sus usuarios. Una vez instalado el caballo de Troya

GAMMA

es prácticamente invisible. No existe ningún medio de prevenirse de "FinFisher" en una máquina infectada.

El software de FinFisher es indetectable por los antivirus estándar. Permite escuchar las conversaciones de Skype, leer los chats y los correos electrónicos cifrados, e incluso encender a distancia la webcam o el micrófono de un ordenador, así como tener acceso a los archivos cifrados presentens en un disco duro. Gamma publicita la capacidad de su software en vídeos comerciales.

Implicaciones en Bahréin

En julio de 2012, algunas informaciones apuntaron a una posible implicación de la tecnología "FinFisher" en Bahréin, donde la situación es particularmente difícil para los infromadores. Muchos de ellos han sido detenidos, encarcelados y torturados, en el contexto de las manifestaciones populares que tienen lugar en el país. La disidente Ala´a Shehabi recibió un correo electrónico infectado, y, sospechando de él, lo transfirió a expertos para su análisis, que detectaron la tecnología "FinFisher" de Gamma. Reporteros Sin Fronteras, el European Center for Constitutional and Human Rights, Privacy Internationale, el Bahrein Center for Human Rights, y Bahrein Watch, pidieron la sede en el Reino Unido de la OCDE profundizar la investigación sobre la implicación de Gamma en Bahréin. Martin Münch, responsable de Gamma, afirma que Bahréin les robó una versión de demostración del software, la modificó y la utiliza actualmente para espiar a periodistas y disidentes. Eric King, director de investigaciones de Privacy Internationale, comenta: "No es fácil integrar FinFisher en la red de un país. Requiere una planificación y un análisis preciso. Por eso es improbable que un país pueda reconfigurar una versión de prueba". Bahrein Watch ha obtenido pruebas de las actualizaciones regulares de los servidores de "FinFisher" de Bahréin, lo que es incompatible con la hipótesis del robo".

Oferta al gobierno egipcio

Durante una búsqueda en el seno de la oficina de una agencia egipcia de informaciones, en 2011, activistas de derechos humanos descubrieron una propuesta de contrato de Gamma para venderle "FinFisher" a Egipto. La empresa niega que se firmara el contrato.

GAMMA

Otras implicaciones

Un estudio reciente de Rapid7, empresa de seguridad informática, ha identificado "FinSpy", el software que asegura el control de "FinFisher", activo en Australia, República Checa, Estonia, Etiopía, Indonesia, Letonia, Mongolia, Catar, Emiratos Árabes Unidos y Estados Unidos. Citizen Lab afirma haberlo encontrado también en otros países. "Hemos descubierto dos servidores en Brunei, uno en el Ministerio Turco de la Comunicación, dos en Singapur, uno en Países Bajos, otros en Indonesia y otro en Bahréin", afirma Citizen Lab, que informa también que algunos de esos servidores se desactivaron cuando se descubrió su existencia.

HACKING TEAM

La empresa italiana Hacking Team describe ella misma sus propias tecnologías como "ofensivas". La empresa ha sido cuestionada por sus ventas a Marruecos y a Emiratos Árabes Unidos. Según ella, el "Remote Control Sytem" que ha desarrollado y que ha nombrado con modestia "Da Vinci", es capaz de romper el cifrado utilizado por correos electrónicos, archivos y protocolos VOIP.

La sociedad

Situada en Milán, propone a las fuerzas del orden soluciones de defensa proactiva en los seis continentes. Emplea a 40 personas en Italia y dispone de oficinas en Annapolis (Estados Unidos) y Singapur. La sociedad se define así: "En Hacking Team pensamos que combatir el crimen debe ser una tarea fácil: Proporcionamos tecnología ofensiva para el mundo entero, eficaz y de simple utilización, destinada a organismo encargados de aplicar la ley y a los servicios de información. La tecnología os debe hacer más fuertes, no impediros".

Expediente

El "Remote Control Sytem" es un "dispositivo furtivo de investigación", destinado a los agentes gubernamentales encargados de hacer cumplir la ley (una tecnología de seguridad agresiva, un software espía, un caballo de Troya, un útil de vigilancia, un útil de ataque, un útil de control de las terminales. En otros términos, es un útil de control de los ordenadores)".

El "Remote Control Sytem", comercializado con el nombre de "Da Vinci", es capaz de romper el cifrado y permitir a la policía y servicios encargados de hacer respetar la ley vigilar archivos y correos electrónicos, incluso los que utilizan la tecnología PGP, las conversaciones de Skype y todos los otros protocolos VOIP, así como la mensajería instantánea. Este sistema hace posible la localización de objetivos e identificación de sus contactos, permite activar a distancia cámaras y micrófonos en todo el mundo; pretende que su software sea capaz de vigilar simultáneamente centenas de millares de ordenadores en un mismo país; sus caballos de Troya pueden infectar windows, mac, linux, iOS, android, symbian y Blackberry.

HACKING TEAM

En el contexto de las comunicaciones digitales modernas, el cifrado de contenidos es muy utilizado par proteger a los usuarios de potenciales escuchas. Pero desgraciadamente el cifrado impide también a los agentes gubernamentales y a los servicios de información controlar ataques y amenazas contra la seguridad de su país. El "Remote Control Sytem" permite burlar este cifrado por medio de un agente de vigilancia instalado directamente sobre el material del objetivo. La recogida de pruebas sobre las máquinas vigiladas es silenciosa y la transmisión de los datos al servidor de "Remote Control Sytem" está cifrada y es prácticamente invisible.

El portavoz de Hacking Team ha indicado, sin entrar en detalles, que la empresa podía vigilar la forma en que su software es utilizado por sus clientes.

Implicaciones en países sensibles

Hacking Team presume de no vender su software a países que violan los derechos humanos. La empresa anuncia que sus productos son utilizados en 30 países de cinco continentes. "El software desarrollado por Hacking Team se vende únicamente a los servicios gubernamentales y jamás a países inscritos en listas negras por Estados Unidos u organizaciones internacionales como la OTAN o la Unión Europea. Un comité independiente compuesto de expertos jurídicos analiza cada venta para asegurar su compatibilidad con nuestra política. Los contratos firmados con los compradores gubernamentales definen los límites de utilización de nuestro software. Vigilamos la actualidad y las comunicaciones públicas, así como los blog y los comentarios en Internet que puedan indicar abusos, y procedemos a investigar si es necesario".

A pesar de estas garantías, lo cierto es que muchos medios de comunicación y expertos en seguridad informática han encontrado rastros del software de Hacking Team en países poco respetuosos con la democracia y los derechos humanos, como lo prueban los siguientes ejemplos:

Implicaciones en Marruecos

Se ha identificado software de Hacking Team en los ordenadores de las oficinas del sito de información marroquí Mamfakinch, unos días

HACKING TEAM

después de que este medio de comunicación recibiera el Breaking Border Award 2012, por Global Voices y Google. Anteriormente ya se había detectado otro en un documento de word que pretendía contener informaciones confidenciales.

Contactado por Reporteros Sin Fronteras para comentar el uso de su software en Marruecos, el portavoz de la empresa no ha negado su presencia en el país. "Tomamos precauciones para asegurarnos que nuestro software no sea utilizado y, en caso negativo, abrimos investigaciones, pero de cualquier forma no revelamos la identidad de nuestros clientes o su localización (respuesta enviada por correo electrónico a Reporteros Sin Fronteras)".

Implicaciones en Emiratos Árabes Unidos

Morgan Marquis-Boire, experto en seguridad, ha examinado documentos adjuntos a un correo electrónico enviado al bloguero Ahmed Mansoor, y ha descubiernto que estaban contaminados, con fuentes sospechas de que la fuente proviniese de Hacking Team. Sus resultados han sido publicados por el Citizen Lab.

TROVICOR

Trovicor es uno de los proveedores más importantes de soluciones legales de interceptación de contenidos en el mundo y pretende equipar a más de 100 países. La sociedad fue interrogada en una audiencia en el Parlamento Europeo, en 2010, sobre su implicación en Irán, en Bahréin y en Siria, donde se encarcelan y torturan regularmente a periodistas e internautas, gracias a la utilización de tecnologías vendidas por sociedades occidentales.

Hasta 2009, Trovicor era conocida por su antiguo nombre, Nokia Siemens Networks (NSN), y "Division for Voice and Data Recording", dentro de "Siemens AGE". Está dirigida por Johann Preinsberger, mediante la sociedad Ickehorn Asset Management, con sede en Munich y filiales conocidas en Suiza, Dubai, Islamabad, Kuala Lumpur y Praga. Tiene un total de 170 empleados.

La sociedad

Creada en 1993, con el nombre de Department for Voice and Data Recording, es uno de los primeros proveedores en el mundo de equipos de vigilancia. Esta antigua división operativa de la empresa alemana Siemens, provee a las autoridades de más de 100 países centros de vigilancia y materiales de interceptación. Desde 2007 está unida a Nokia Siemnes Networks y, en 2009, fue cedida a una sociedad de gestión llamada Trovicor, que se comprometió a mantener los contratos de Nokia Siemens Network. Fue el principal e sponsor del mayor salón de exposición del mundo de materiales de vigilancia y censura, el ISS World MEA 2013, de Praga.

Barry French, un representante de Nokia Siemens Network, explicó, en una ponencia en el Parlamento Europeo, que "los centros de vigilancia son, desde nuestro punto de vista, más inquietantes (que los equipos de interceptación legal) y levantan más problemas relacionados con los derechos humanos que no estamos en condiciones de tratar. Nuestra competencia no es trabajar con los organismos de aplicación de la ley, que no son nuestros clientes habituales. Estos organismo podrían tener interés en extender las funciones de los centros de vigilancia más allá de los niveles estándar de interceptación legal".

Numerosos elementos permiten sostener la tesis de una colaboración entre Trovicor y otras

TROVICOR

sociedades, que le proporcionarían soluciones como los caballos de Troya. Las herramientas de Trovicor se basan en sistemas innovadores desarrollados por la empresa y están pensadas para integrar las soluciones más efectivas, proporcionando así una plataforma flexible para detener a criminales.

Expediente

Los centros de vigilancia de Trovicor son capaces de interceptar todas las comunicaciones estándar del European Telecommunications Standards Institute (ETSI), es decir, las llamadas telefónicas, los servicios de mensajes de texto, las llamadas VOIP, así como el tráfico en Internet. Sin embargo, no pueden espiar datos almacenados en discos duros. Trovicor propone soluciones de tratamiento de grandes cantidades de datos gracias a Intelligent Platforms. La empresa pone también ofrece un programa de evaluación de la red y de la estructura de Internet en un país, para ofrecer soluciones de vigilancia a medida, así como formaciones adaptadas a las autoridades (LifecCicle Management). En caso de fracaso, asegura el mantenimiento del sistema y el desarrollo de opciones sobre el material instalado.

Implicaciones en Bahréin

Según diversos medios de comunicación y organizaciones de defensa de los derechos humanos, Bahréin tiene centros de vigilancia que han conducido a la prisión y tortura de periodistas y activistas. Fuentes anónimas de Trovicor (que trabajaban antes para Siemens) han confirmado que ésta vendió equipos en 2006 y que Trovicor aseguró su mantenimiento. En sesiones de tortura a prisioneros, como Abd Al Ghani Khanjhar, les fueron mostradas comunicaciones privadas, como SMSs, correos electrónicos y conversaciones telefónicas. Estos elementos han sido manifiestamente obtenidos por el programa de interceptación de contenidos que tiene Bahréin.

El European Center for Constitutional and Human Rights, Privacy international, el Bahrein Center for Human Rights, Bahrein Watch, y Reporteros Sin Fronteras llevaron a Trovicor ante las instancias alemanas de la OCDE para que investigasen el papel de la empresa en Bahréin.

TROVICOR

Implicaciones en Irán

En 2009, Nokia Siemens Network proporcionó equipos a las autoridades iraníes, y, cuando la empresa suspendió la venta de sus centros de vigilancia, Trovicor continuó asegurando el mantenimiento de los ya implantados.

Nokia Siemens Network sigue presente en Irán, donde asiste a las redes de teléfonos móviles. La empresa anunció, a finales de 2011, que ponía fin a sus actividades en el país.

Otras implicaciones

Según informes de diversos medios de comunicación, en 2000 y en 2008, Trovicor proporcionó centros de vigilancia a Siria.

Se sospecha que Yémen también ha comprado centros de vigilancia a Trovicor. En 2010, la empresa pidió la protección de su marca en el país, lo que muestra que Trovicor tiene intereses allí.

Trovicor tiene una filial oficial en Kuala Lumpur y, en 2009, la empresa pidió una protección de su marca en el espacio económico malasio.

En Alemania, Trovicor proporciona equipos de interceptación legal para la policía de Baviera.