ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

34/2014 4 abril de 2014

Adolfo Hernández Lorente
Enrique Fojón Chamorro
*Guillem Colom Piella**

VIGILADOS POR DEFECTO

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

VIGILADOS POR DEFECTO

Resumen:

El escándalo Snowden no sólo ha puesto de manifiesto el programa de ciberespionaje masivo realizado por Estados Unidos sobre sus aliados y potenciales adversarios; sino también la vigilancia por defecto (*surveillance by default*) que puede estar integrada de fábrica en una gran cantidad de tecnologías que utilizamos en nuestras vidas diarias. Este documento de opinión pretende poner de manifiesto este hecho y sus posibles implicaciones para nuestras sociedades.

Abstract:

The Snowden scandal has not only revealed the massive cyberspionage performed by the United States against its allies and potential adversaries; but also the surveillance by default capabilities integrated in a number of technologies we use in our daily lives. This document is aimed at exposing this fact and its possible effects to our societies.

Palabras clave:

Vigilancia por defecto, ciberespionaje, ciberseguridad, Agencia de Seguridad Nacional, Estados Unidos, Filtraciones, Aldea global, servicios de inteligencia.

Keywords:

Surveillance by default, cyberspionage, cybersecurity, National Security Agency, United States, Filtrations, Global Village ,intelligence services.

Adolfo Hernández Lorente Enrique Fojón Chamorro
Guillem Colom Piella

"Nuestros aliados de hoy serán los enemigos del mañana,
aprendamos lo máximo mientras sigan siendo nuestros aliados
ya que no será posible cuando sean nuestros enemigos"
Coronel Carter Clarke

INTRODUCCIÓN

Corría el año 1973, en el transcurso de una reunión de trabajo entre el Reino Unido y la República Popular China celebrada en Beijín, el Presidente chino Mao Tse Tung preguntó al Primer Ministro británico Edward Heath por el "sinsentido" del escándalo Watergate y la delicada situación en la que se encontraba el Presidente estadounidense Richard Nixon tras haberse destapado las escuchas ilegales a la oposición política. Heath replicó a Mao que a qué se refería exactamente con "sinsentido" y éste contestó en los siguientes términos: *"Se acusa a Nixon de haber utilizado micrófonos ocultos para espiar a sus rivales, ¿no? Pero, todos los usamos, ¿verdad? Además, todo el mundo lo sabe, así que no sé a qué viene tanto revuelo"*[1].

Hoy en día, el imparable avance tecnológico, y en especial la popularización del acceso a Internet desde una amplia gama de dispositivos (desde los clásicos ordenadores de sobremesa y portátiles hasta una amplia gama de dispositivos móviles como *smartphones* o *tablets*), ha permitido que muchos ciudadanos de casi cualquier país del globo tengan acceso a un volumen de información, comunicación y servicios que antes eran completamente inimaginables. No obstante, estos mismos desarrollos también han permitido a los gobiernos – tanto autoritarios como democráticos – obtener unas capacidades de vigilancia masiva de sus ciudadanos que hasta hace muy poco tiempo sonaban a ciencia ficción.

En efecto, el reciente escándalo de la Agencia Nacional de Seguridad estadounidense (*National Security Agency* – NSA) ha puesto de manifiesto el férreo control que los gobiernos pueden ejercer sobre Internet, sobre los contenidos que en ella discurren y sobre las actividades de los individuos que lo utilizan[2]. A pesar de que Estados Unidos es el país que dispone de las cibercapacidades más avanzadas del planeta, son muchas las naciones que están invirtiendo vastos recursos con el fin de obtener capacidades cibernéticas que les permitan controlar de manera eficaz y eficiente sus ciberespacios nacionales específicos.

[1] Edward Heath: *The Course of My Life: My Autobiography*, Londres: Dumpton Gap & Co., 1998, p. 473.

[2] Aunque existe una amplia bibliografía al respecto, a tal efecto véase: Peter W Singer y Allan Friedman: *Cybersecurity and Cyberwar*, Nueva York: Oxford University Press, 2014 o Richard Clarke y Robert K. Knake: *Cyber War*, Nueva York: Harper Collins, 2010.

Ejemplos representativos de ello pueden ser países como China, Irán, Rusia o numerosos regímenes árabes y asiáticos, que utilizan el ciberespacio como una importante herramienta para monitorizar las actividades y comunicaciones de sus ciudadanos y así poder controlar a la oposición política y dificultar la movilización social. Los ejemplos de este último caso son numerosos y variados, comprendiendo desde la tradicional monitorización de los perfiles de *Facebook* y *Twitter* hasta los cortes de Internet que se produjeron durante las Primaveras Árabes; la proliferación de perfiles sociales virtuales y la guerra informativa en el ciberespacio entre Rusia y Ucrania durante la crisis de Crimea o la determinación del gobierno turco de clausurar el acceso a la red social virtual *Twitter*[3].

EL ESCÁNDALO DE LA NSA

A lo largo de sus sesenta años de historia[4], la NSA se ha visto implicada en numerosos escándalos de espionaje masivo a ciudadanos, gobiernos, organismos internacionales, sedes diplomáticas o empresas, realizadas tanto dentro como fuera del territorio estadounidense y de manera indiscriminada contra aliados o enemigos del país[5].

En el año 1975, las referencias a la NSA aparecidas en las transcripciones de algunos de los comparecientes ante la *Comisión Rockefeller* – impulsada por el Congreso para investigar las actividades ilícitas de la Agencia Central de Inteligencia (CIA) en territorio estadounidense[6] –

[3] James Reynolds: "Twitter website 'blocked' in Turkey" en *BBC* (21 de marzo de 2014), en: http://www.bbc.com/news/world-europe-26677134

[4] Recuérdese que la NSA es una organización de inteligencia criptológica fundada en 1952 para apoyar al Departamento de Defensa estadounidense. Constituida a raíz de las demoledoras conclusiones de la Comisión Brownlee – que alertaba de la incapacidad del país para interceptar las comunicaciones cifradas del bloque oriental, lo que había impedido prever el bloqueo de Berlín, anticipar el inicio de la Guerra de Corea o conocer las actividades de los contendientes durante el conflicto – ésta reemplazó a la efímera Agencia de Seguridad de las Fuerzas Armadas, constituida cuatro años antes para coordinar las actividades de inteligencia electrónica y de comunicaciones del país.

[5] En efecto, la historia reciente de la NSA – o al menos la que se conoce – ha estado marcada por sonados escándalos, fracasos o filtraciones, entre los que destacan la escucha de las comunicaciones de personalidades contrarias a la Guerra de Vietnam o promotoras de los derechos civiles en la década de 1960; los incidentes de los buques espía *USS Liberty* en la costa israelí en la Guerra de los Seis Días (1967) y el *USS Pueblo* en las costas norcoreanas poco antes de iniciarse la ofensiva del Tet (1968); la imposibilidad de localizar a los responsables de los atentados del 11-S, a pesar de que algunos residían de forma permanente en Estados Unidos y la mayoría de ellos vivieron en Laurel, a pocos kilómetros de la sede central de la agencia en Fort Meade (Maryland); la imposibilidad de proporcionar a George W. Bush evidencias suficientes sobre la existencia o desarrollo de armamento de destrucción masiva en Irak; o la reciente filtración realizada por Edward Snowden.

[6] Esta comisión descubrió tanto los nexos de unión entre la CIA y la NSA como el espionaje sistemático de ésta última sobre las comunicaciones de ciudadanos estadounidenses y extranjeros en suelo americano, lo que obligó al director de la NSA a declarar ante el Congreso y desvelar parte de las actividades de la agencia, entre las que se hallaba la monitorización de las comunicaciones de activistas de los derechos civiles y personalidades contrarias a la Guerra de Vietnam. Este escándalo motivó la aprobación del *Foreign Intelligence Surveillance Act* (FISA), una ley decretada en 1978 y todavía en vigor que prohíbe expresamente espiar a ciudadanos estadounidenses dentro del país.

y el posterior artículo publicado por el periódico *New York Times* bajo el evocador título "La Agencia de Seguridad Nacional acusada de espiar la mayoría de las comunicaciones privadas"[7] sacarían a la NSA de su anonimato. Y es que durante las tres décadas – entre los años 1945 y 1975 – que estuvo vigente la *Operación Shamrock*, la inmensa mayoría de los telegramas que entraban y salían de Estados Unidos eran interceptados, copiados y posteriormente enviados a sus destinatarios legítimos fuera del país. Evidentemente, ello fue posible gracias a la participación de las tres grandes compañías telegráficas de la época: *ITT World Communications*, *RCA* y *Western Union*, que colaboraron activamente con la agencia, proporcionándole acceso directo a todas las comunicaciones y ocultando este hecho a la opinión pública.

Fue precisamente a raíz de esta situación cuando la NSA estadounidense y su homólogo británico, el Cuartel General de Comunicaciones Globales (*Global Communications Headquarters* – GCHQ), estrecharon sus lazos de colaboración. Coincidiendo con el comienzo de la segunda Guerra Fría a finales de la década de 1970, la conexión existente entre el presidente Ronald Reagan y la primera ministra Margaret Thatcher y la consolidación de la revolución de la información, Washington y Londres comenzaron a poner en común sus recursos tecnológicos, infraestructuras de escucha, medios de procesamiento y productos de inteligencia, posibilitando un intercambio fluido y efectivo de información entre ambas potencias que ha permanecido intacto hasta la fecha de hoy. Precisamente, el nivel de cooperación entre estos dos países es tan estrecho que no sólo se han firmado convenios de colaboración absoluta entre la NSA y el GCHQ (algo que no existe con ningún otro país del grupo de los *cinco ojos* compuesto por Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos); sino que también éste último ha sido el responsable de realizar las copias de seguridad (*backups*), monitorizar las comunicaciones o procesar la información cuando en Fort Meade se producían largos apagones – de dos o tres días de duración – durante el incremento en la demanda de procesamiento de datos, sobre todo a partir del 11-S.

A principios del año 2002 el Presidente George W. Bush, todavía bajo el shock de los ataques terroristas del 11 de Septiembre de 2001, autorizaba, bajo las intensas presiones del General Michael Hayden (director de la NSA entre los años 2000 y 2005) y de su Vicepresidente Dick Cheney, a la NSA a monitorizar, almacenar y analizar sin orden judicial previa, las llamadas telefónicas y los correos electrónicos de todos aquellos ciudadanos, estadounidenses o no, sospechosos de tener algún nexo de unión con la organización terrorista Al-Qaeda. Un año después, amparándose en esta orden presidencial, los servicios de inteligencia estadounidenses espiaron las llamadas telefónicas y correos electrónicos de los

[7] Nicholas M. Horrocic: "National Security Agency reported eavesdropping on most private cables", en *New York Times* (31 de agosto de 1975), en: http://jfk.hood.edu/Collection/Weisberg%20Subject%20Index%20Files/N%20Disk/National%20Security%20Agency/Item%2007.pdf

representantes de los países miembros del Consejo de Seguridad de las Naciones Unidas durante los días previos a la votación de la Resolución 1441 (2002) que supuestamente debía autorizar la guerra de Irak[8]. Además, tal y como ha revelado Edward Snowden, las labores de espionaje acabaron generalizándose a muchos otros países, organizaciones internacionales o líderes políticos de todo el globo con independencia de si éstos eran aliados o potenciales adversarios de Washington.

A finales de 2005, dos periodistas estadounidenses ya denunciaron la autorización a la NSA por el Presidente Bush en 2002 a través de la cual se permitía a la agencia eludir el cumplimiento del *Foreign Intelligence Surveillance Act* (FISA), que prohíbe expresamente espiar a ciudadanos estadounidenses dentro del país[9]. A mediados de 2013, el periódico británico *The Guardian* publicaba parte de los más de 20.000 documentos sensibles o clasificados sustraídos por Edward Snowden, ex-contratista de la CIA y la NSA de la sede hawaiana de la agencia. Este escándalo provocó que muchos aliados, socios y potenciales adversarios de Estados Unidos solicitaran explicaciones a Washington: el ciberespionaje y la vigilancia por defecto habían pasado a ocupar la atención informativa y muchos gobiernos de la comunidad internacional que hasta ahora incluían al ciberespacio y su seguridad y defensa en su agenda política alcanzaban a comprender su importancia estratégica.

El pasado 17 de enero de 2014, asaltado por las críticas a su programa de inteligencia de señales (SIGINT) y por el malestar y la desconfianza que provocó entre sus aliados el programa PRISM de ciberespionaje masivo, el Presidente Barack H. Obama compareció públicamente desde el Departamento de Justicia para enumerar y explicar a sus compatriotas, y al resto de la comunidad internacional, las medidas que su administración adoptará para controlar las actividades SIGINT del sistema nacional de inteligencia de los Estados Unidos[10].

Aun defendiendo la legitimidad y legalidad de sus programas, el presidente Obama se comprometió a ejecutar un conjunto de reformas en los próximos meses; recogidas éstas en la Directiva Política Presidencial 28 (*Presidential Policy Directive 28 – Signals Intelligence Activities, PPD-28*)[11], Obama anunció que dejara de espiar a los líderes de países aliados y

[8] En este sentido, téngase en cuenta que fue a raíz de los sucesos del 11-S cuando, amparada en la Guerra contra el Terror y la nueva legislación antiterrorista, la NSA puso en marcha numerosos programas de vigilancia tecnológica capaces de monitorizar de forma exhaustiva el tráfico de Internet, las cuentas de correo electrónico, los datos multimedia, las comunicaciones telefónicas o la telefonía por Internet, siendo el más famoso de ellos el controvertido PRISM capaz de monitorizar el ciberespacio.

[9] James Risen & Eric LitchBlau: "Bush Lets U.S. Spy on Callers Without Court's", en *New York Times* (16 de diciembre de 2005), en: http://www.nytimes.com/2005/12/16/politics/16program.html

[10] Enrique Fojón: "El ciberpoder de Obama", en *Elcano Blog* (21 de enero de 2014), en: http://www.blog.rielcano.org/el-ciberpoder-de-obama

[11] Office of the President of the United States: *Presidential Policy Directive 28 –Signals Intelligence Activities,*

pondrá límites a los procesos de obtención de información de los servicios de inteligencia del país haciéndolos compatibles con los derechos civiles y la privacidad de los ciudadanos estadounidenses y del resto del mundo.

Sin embargo, estas reformas no supondrán un menoscabo de las capacidades SIGINT del sistema de inteligencia de los Estados Unidos. En cualquier caso, el posicionamiento del presidente Obama ha sido contundente: Estados Unidos no dejará de utilizar sus capacidades cibernéticas, de forma que la Administración no planea interrumpir sus actividades de inteligencia electrónica.

Resulta pertinente recordar que se estima que aproximadamente el 80% de la inteligencia que emplea la administración estadounidense para apoyar sus decisiones políticas provienen del ciberespacio.

De esta forma, si a raíz de las filtraciones de Edward Snowden de mayo del pasado año se evidenciaba la existencia de ambiciosos programas de recolección y tratamiento digital de información conformando una compleja trama de espionaje masivo y una elaborada red de colaboración público-privada en el entorno estadounidense[12]; en el *Chaos Communications Congress* – organizado por el famoso Chaos Computer Club, la mayor asociación de hackers de Europa– celebrado en Hamburgo a finales de 2013, Jacob Appelbaum, investigador de seguridad informática y miembro destacado de Wikileaks, arrojó una nueva aproximación detallada de las técnicas que la NSA utiliza en sus actividades de vigilancia.

Los documentos compartidos por Appelbaum y el periódico alemán *Der Spiegel* revelan que la NSA puede acceder a casi cualquier dispositivo "desde fábrica" o "por defecto", haciendo patente la existencia de un catálogo de "puertas traseras" (*backdoors*) para numerosos dispositivos hardware de usuario final o de uso empresarial[13].

Washington DC. U.S. Government Printing Office (17 de enero de 2014), en: http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

[12] En este sentido, véase: Enrique Fojón; Adolfo Hernández y Guillem Colom: "La Agencia de Seguridad Nacional (NSA): espionaje y colaboración público-privada en EEUU", en *Análisis del Real Instituto Elcano* nº 41 (11 de noviembre de 2013), en: http://www.realinstitutoelcano.org/wps/wcm/connect/ARI41-2013-THIBER-NSA-espionaje-publico-privada-Snowden.pdf

[13] Jacob Appelbaum, Judith Horchert y Christian Stöcker: "Shopping for Spy Gear: Catalog Advertises NSA Toolbox", en *Der Spiegel* (29 diciembre 2013), en: http://www.spiegel.de/international/world/ catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html; o Jacob Appelbaum, Laura Poitras, Marcel Rosenbach, Christian Stöcker, Jörg Schindler and Holger Start: "Inside TAO: Documents Reveal Top NSA Hacking Unit", en *Der Spiegel* (29 de diciembre de 2013), en: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html.

EL CATÁLOGO ANT

El catálogo ANT es un documento clasificado de cincuenta páginas editado en 2008 en el que se listan las tecnologías de soporte en la vigilancia cibernética a disposición de la unidad de élite TAO[14] (*Tailored Access Operations*) de la NSA. En los casos en los que los métodos de hacking y skimming de datos, habituales en los operativos ejecutados por el TAO, no son suficientes, interviene el catálogo ANT con sus herramientas específicas, que permiten penetrar en los equipos de red, realizar seguimientos de teléfonos móviles y PCs y desviar o incluso modificar los datos en tránsito en la red. Los *implants*, como se les conoce en la jerga de la NSA a estos dispositivos y técnicas, han desempeñado un papel considerable en la capacidad de las agencias de inteligencia para establecer una red encubierta global de cibervigilancia.

Según Der Spiegel, *"…la lista se asemeja a un catálogo de venta por correo, en el cual los empleados de la NSA pueden adquirir las tecnologías de la división ANT para obtener información de sus objetivos"*[15]. Los precios de los artículos del catálogo oscilan entre unos pocos cientos de dólares a cantidades cercanas a los dos cientos cincuenta mil dólares[16].

Estos datos evidencian, una vez más, la sofisticación del entramado de colaboración público-privada que mantienen las agencias estadounidenses de inteligencia con empresas del sector tecnológico. Pero, ¿cómo puede la NSA introducir "de fábrica" los mencionados implantes?

De una parte, la división TAO interceptó las entregas y envíos de ordenadores y portátiles por todo el mundo con el fin de instalar *spyware* e implantes físicos en los dispositivos *hardware*[17]. Aparentemente, esto fue posible tras una estrecha cooperación con el FBI y la

[14] En este sentido, TAO se halla encuadrado en la dirección de Inteligencia de Señales de la NSA, está compuesto por hackers de primer nivel y su función primordial es la explotación de los sistemas de información y comunicaciones del adversario.

[15] Jacob Appelbaum, Judith Horchert y Christian Stöcker: "Shopping for Spy Gear: Catalog Advertises NSA Toolbox", en *Der Spiegel* (29 de diciembre de 2013), en: http://www.spiegel.de/international/world/ catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

[16] Courtney Subramanian: "The TAO of the NSA: Specialized Hacking Team Gets the 'Ungettable'", en *Time* (29 de diciembre de 2013), en: http://world.time.com/2013/12/29/the-tao-of-the-nsa-specialized-hacking-team-gets-the-ungettable.

[17] Erik Kain; "NSA Intercepting Laptops Ordered Online, Installing Spyware", en *Forbes* (29 de diciembre de 2013), en: http://www.forbes.com/sites/erikkain/2013/12/29/report-nsa-intercepting-laptops-ordered-online-installing-spyware.

CIA, como han declarado a *The Guardian* funcionarios de la NSA: *"TAO es un activo de seguridad nacional único que está en la primera línea de la NSA con el objetivo de defender los intereses de la nación y sus aliados, estando su trabajo centrado en la explotación de los datos digitales y comunicaciones como apoyo en las tareas de recopilación de inteligencia en el extranjero"*[18].

Pero la NSA no se detiene en la mera interceptación de envíos de *hardware*. Algunos de los implantes detectados son hardware propio diseñado *ex profeso* a tal efecto. Dada la extensión de la máquina de vigilancia de la NSA hasta el momento existe una gran variedad de dispositivos utilizados por la Agencia.

La tabla de la página siguiente muestra una relación detallada de los diversos implantes identificados, tanto software como hardware, mostrando su coste individual (en dólares americanos) así como los fabricantes asociados.

Los implantes que se describen en la tabla están dirigidos principalmente a los productos fabricados por empresas estadounidenses, si bien no hay una referencia explícita en el documento que sugiera la existencia de un marco de colaboración entre dichas organizaciones y las agencias de inteligencia norteamericanas.

Esta vinculación público privada, apriorísticamente indirecta, mostrada de nuevo tras la publicación del catálogo ANT, junto con el fallo del juez Richard Leon que forzó al Departamento de Justicia estadounidense a estudiar el recurso de inconstitucionalidad sobre las técnicas SIGINT de la NSA, provocó que un grupo de directivos de las principales empresas tecnológicas de Estados Unidos instaran al presidente, Barack Obama, y al vicepresidente, Joe Biden, a que se actúe de forma efectiva para impulsar cambios en el seno de la Agencia, limitando la vigilancia a los ciudadanos y convirtiéndose en una referencia para los aliados en esta materia.

[18] Joanna Walters: "NSA 'hacking unit' infiltrates computers around the world – report", en *The Guardian* (29 de diciembre de 2013), en: http://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao.

CATÁLOGO DE IMPLANTS DE LA DIVISIÓN TAO DE LA NSA

ÁMBITO APLICACIÓN	COSTE	NOMBRE	DESCRIPCIÓN	FABRICANTES
ORDENADORES SOBREMESA	10.740$	FIREWALK	Dispositivo idéntico a un RJ45 estándar que permite que los datos en tránsito sean monitorizados o inyectados, a través radiofrecuencia. Empleado, por ejemplo, para crear una VPN en el equipo destino	HARDWARE PROPIO
	-$	GINSU	Implante que permite el control remoto de un dispositivo con bus PCI	MICROSOFT
	-$	IRATEMONK	Implante oculto en el firmware de discos duros que reemplaza el MBR	Western Digital, Seagate, Maxtor, Samsung
	-$	SWAP	Tecnología que mediante la BIOS de los sistemas operativos FreeBSD, Linux, Solaris o Windows permite el control remoto de los mismos	MICROSOFT, LINUX, FREEBSD, ORACLE
	-$	WISTFULTOLL	Implante software que emplea el Windows Management Instrumentation (WMI) para acceder a la inforamación	MICROSOFT
	750$	HOWLERMONKEY	transceptor de radiofrecuencia que permite (en combinación con otros implantes) extraer datos de los sistemas o controlarlos remotamente	HARDWARE PROPIO
	20$	COTTONMOUTH I	Una familia de conectores USB y Ethernet modificados para instalar troyanos y trabajar como puentes inalámbricos, proporcionando acceso remoto encubierto en la máquina de destino	HARDWARE PROPIO
	4.000$	COTTONMOUTH II		
	25$	COTTONMOUTH III		
	N/E	JUNIORMINT	Diminuto implante hardware basado en un módulo multichip (MCM) para diferentes usos	VARIOS
	3.500$	MAESTRO II	Implante hardware del tamaño de una moneda basado en un módulo multichip (MCM) que sirve como núcleo en otros implantes	HARDWARE PROPIO
	625$	TRINITY	Implante hardware del tamaño de una moneda basado en un módulo multichip (MCM) que sirve como núcleo en otros implantes	HARDWARE PROPIO
	50.000$	SOMBERKNAVE	Implante software para Windows XP que permite ser controlado de forma remota desde la sede de la NSA	MICROSOFT
	30$	SURLYSPAWN	Monitor de teclado que emite las teclas pulsadas de forma remota (radio) en equipos que no están conectados a Internet	HARDWARE PROPIO
	30$	RAGEMASTER	Dispositivo de interceptación de vídeo entre la salida VGA de un ordenador y la tarjeta de vídeo.	HARDWARE PROPIO
SERVIDORES	-$	IRONCHEF	Implante en la BIOS de los servidores Proliant de HP empleado para comunicar con la NSA a través de un hardware oculto	HP
	-$	DEITYBOUNCE	Implante en la BIOS de los servidores PowerEdge de Dell empleado para comunicar con la NSA	DELL
FIREWALLS	-$	JETPLOW	Instala una puerta trasera persistente a través del firmware en los firewalls Cisco PIX y ASA	CISCO
	N/E	HALLUXWATER	Instala una puerta trasera software en la ROM en los firewalls Eudemon de Huawei	HUAWEI
	N/E	FEEDTROUGH	Instala una puerta trasera software en los modelos N5XT, NS25, NS50, NS200, NS500, ISG100	JUNIPER
	-$	GOURMETTROUGH	Implante configurable para diversos modelos Juniper	JUNIPER
	-$	SOUFLETROUGH	Implante BIOS para Juniper SSG300 y SSG 500	JUNIPER
DISPOSITIVOS DE ESCUCHA	30$	LOUDAUTO	Implante pasivo de audio para la retransmisión de conversacionesa través de reflexiones radar	HARDWARE PROPIO
	N/E	NIGHTWATCH	Ordenador portátil utilizado para reconstruir y visualizar datos de vídeo de señales errantes, que se utiliza en conjunción con una fuente de radar como el CTX4000 para iluminar el objetivo con el fin de recibir datos de él	HARDWARE PROPIO
	N/E	CTX4000	Dispositivo de radar de onda continua que puede recoger información de un sistema de destino no conectado a la red	HARDWARE PROPIO
	40.000$	PHOTOANGLO	Proyecto conjunto de la NSA y el GCHQ para desarrollar un sistema de radar que remplace el CTX4000	HARDWARE PROPIO
	30$	TAWDRIYARD	Dispositivo que refleja las ondas de radar de forma que permite localizarlo exactamente en una habitación, incluso a través de los muros	HARDWARE PROPIO
DISPOSITIVOS MÓVILES		PICASSO	Implante software que recupera la ubicación del teléfono, accede a los metadatos y al micrófono a través de SMS o del USB del teléfono	VARIOS
	-$	DROPOUTJEEP	implante de software para el iPhone de Apple que utiliza aplicaciones para aportar funciones específicas SIGINT, comola capacidad de captar o inyectar archivos del dispositivo, recuperar SMS, lista de contactos, contestador automático, geolocalización, micrófono, captura de la cámara, geoposicionamiento	APPLE
	-$	GOPHERSET	Software GSM que utiliza la API de la tarjeta SIM de un teléfono (SIM Toolkit o STK) para controlar el teléfono de forma remota	VARIOS
	-$	MONKEYCALENDAR	Software que transmite la ubicación de un teléfono móvil a través de mensajes de texto oculto	VARIOS
	N/E	TOTECHASER	Implante software instalado en la flashroom de los teléfonos satélite Thruaya 2520 que filtra información a través de SMS	THURAYA
	0	TOTEGHOSTLY 2.0	Softwarepara teléfono móvil Windows que permite un control remoto completo	MICROSOFT
	40.000$	CANDYGRAM	Dispositivo que emula una torre de teléfono móvil GSM	HARDWARE PROPIO
	4.000$	CROSSBEAM	Implante software similar a un módulo GSM que permite interceptar las comunicaciones y acceder de forma remota	VARIOS
	25.000$	NEBULA	Simulador de redes GSM 2G y 3G para interceptación	HARDWARE PROPIO
	N/E	THYPON HX	Simulador de cualquier red mundial para interceptación	HARDWARE PROPIO
	15.000$	GENESIS	Teléfono móvil modificado que permite posicionar a un teléfono, frecuencias empleadas y parámetros de red	HARDWARE PROPIO
	70.000$	ENTOURAGE	Hardware que permite posicionar a un teléfono usando la red GSM y 3G	HARDWARE PROPIO
	40.000$	EBSR	Simulador de red GSM que permite interceptar comunicaciones en la banda de 900/1800/1900 MHz	HARDWARE PROPIO
	N/E	WATERWITCH	Hardware que permite posicionar a un teléfono usando la red GSM y 3G	HARDWARE PROPIO
	70.000$	CYCLONE HX9	Simulador de red GSM que permite interceptar comunicaciones en la banda de 900 MHz	HARDWARE PROPIO
REDES INALÁMBRICAS	VARIABLE	NIGHTSTAND	Sistema portáti de explotación de vulnerabilidades que se instala de forma inalámbrica (estándar 802.11) en entornos Microsoft Windows desde una distancia de hasta 13 kms	MICROSOFT
	6.000$	SPARROW II	Pequeño dispositivo para mapear redes WIFI, por ejemplo, siendo introducido en un vehículos aéreo no tripulado (UAV)	HARDWARE PROPIO
ROUTERS	N/E	HEADWATER	Instala una puerta trasera persistente basada en software en la ROM que permite el control remoto del dispositivo	HUAWEI
	N/E	SCHOOLMONTANA	Puerta trasera software resistente a actualizaciones aplicable a la serie J de Juniper	JUNIPER
	N/E	SIERRAMONTANA	Puerta trasera software resistente a actualizaciones e implantado en la BIOS aplicable a la serie M de Juniper	JUNIPER
	N/E	STUCCOMONTANA	Puerta trasera software resistente a actualizaciones e implantado en la BIOS aplicable a la serie T de Juniper	JUNIPER

FUENTE: Elaboración propia en base a la información publicada por el periódico alemán *Der Spiegel*

Independientemente del modo, la eficacia de los implantes del heterogéneo catálogo ANT radica en la inclusión de puertas traseras "de fábrica", dificultando la detección por parte del sujeto bajo vigilancia. A modo ilustrativo, tras la publicación de Applebaum, se reveló que la NSA dispone de la capacidad de inyectar software malicioso en dispositivos iPhone usando un producto ANT llamado DROPOUTJEEP[19]. Como consecuencia, Apple emitió recientemente un comunicado negando cualquier conocimiento previo de dicho spyware manifestando que iban a *"tomar medidas para proteger su sus clientes ante ataques de seguridad independientemente de quién esté detrás de ellos"*[20].

CONCLUSIONES

El "escándalo Snowden" ha revelado la intrincada, compleja y omnipresente red de espionaje tecnológico articulada por Washington para proporcionar inteligencia al país y mantener el liderazgo en la dimensión cibernética. Para posibilitar las labores de la NSA, muchas empresas privadas – desde proveedores de servicios de Internet hasta fabricantes de hardware o desarrolladores de software – han colaborado de manera voluntaria con la agencia (con casos tan sonados como los gigantes *Microsoft*, *Apple*, *Google* o *Facebook* u operadoras como *Verizon*, *AT&T*, *Comcast* o *AOL*). De manera similar, otras empresas de estos sectores también se vieron forzadas a colaborar con la NSA por orden judicial, y las que no lo hicieron se vieron abocadas al cierre tal y como sucedió con los proveedores de correo seguro *Lavabit*[21] y *Silent Circle*[22].

Y si ello no fuera suficiente, la NSA también dispone de capacidades especializadas que le permiten acceder de manera encubierta a cualquier red, equipo o sistema mediante la explotación de las debilidades inherentes de las infraestructuras de Información y Telecomunicaciones, los equipos de hardware o los sistemas de software.

En estos últimos casos, si la aproximación de los implantes listados en el catálogo ANT denota una sofisticación sin parangón, es igualmente preocupante el hecho de que Applebaum está poniendo de relieve un documento clasificado filtrado hace más de seis años. En ese momento, la NSA probablemente no disponía de las cibercapacidades que se

[19] Erik Kain: "The NSA Reportedly Has Total Access To The Apple iPhone", en *Forbes* (30 de diciembre de 2013), en: http://www.forbes.com/sites/erikkain/2013/12/30/the-nsa-reportedly-has-total-access-to-your-iphone

[20] Neil Hughes: "Apple says it was unaware of NSA's iPhone spying, vows to defend customers' privacy", en *Apple Insider* (31 de diciembre de 2013), en: http://appleinsider.com/articles/13/12/31/apple-says-it-was-unaware-of-nsas-iphone-spying-vows-to-defend-customers-privacy

[21] **Dominic Rushe: "Lavabit founder refused FBI order to hand over email encryption keys", en *The Guardian* (3 de octubre de 2013), en: http://www.theguardian.com/world/2013/oct/03/lavabit-ladar-levison-fbi-encryption-keys-snowden**

[22] **Jon Russell: "Silent Circle follows Lavabit in closing its encrypted email service because it's 'better to be safe than sorry'", en *TNW* (9 de agosto de 2013), en: http://thenextweb.com/insider/2013/08/09/silent-circle-follows-lavabit-in-closing-its-encrypted-email-service-because-it-cannot-be-secure/**

han demostrado con las filtraciones de Snowden. Quién sabe de qué capacidades de vigilancia dispone en la actualidad…

Este conjunto de descubrimientos no sólo ha generado enormes controversias en la opinión pública mundial; sino que también ha provocado que muchos gobiernos u organizaciones internacionales, temerosos del alcance y capacidades de la red de espionaje electrónico estadounidense, se planteen la necesidad de fabricar su propio hardware, desarrollar su propio software y hasta incluso tender sus propias redes de telecomunicaciones para tratar de impedir el acceso de la NSA a sus comunicaciones[23]. Y es que la inmensa mayoría de los 900.000 kilómetros de cables submarinos que recorren todo el planeta y que permiten nuestras conexiones a Internet tienen sus puntos de entrada y salida en el Reino Unido – donde el GCHQ no sólo podrá monitorizar los flujos de información, sino también compartirlos con la NSA[24] – o en las costas Este y Oeste de Estados Unidos, donde la Agencia tiene infraestructuras, capacidades o convenios de escucha. Evidentemente, esto significa que estos dos países no sólo pueden controlar el grueso – se asume que más del 90% – del tráfico mundial de datos, sino también utilizar la información que por allí discurre para obtener ventaja en el ámbito político, estratégico, militar, industrial o comercial.

En conclusión, la vigilancia por defecto o de fábrica desarrollada por muchos gobiernos es cada vez más evidente y común, y no sólo entre estados autoritarios tal y como tradicionalmente asumía la opinión pública. Este proceso de normalización y aceptación social que se está produciendo hace que la vigilancia masiva esté imbricada en nuestra vida cotidiana, siendo la ciudadanía y las empresas cada vez más ajenas e indolentes ante ello. El concepto de privacidad está desapareciendo, convirtiéndose en una reliquia garantista del pasado ante el nivel de interconexión masivo y el nuevo concepto de “aldea global”.

i

Adolfo Hernández Lorente
Enrique Fojón Chamorro
*Guillem Colom Piella**
THIBER, the cybersecurity think tank

[23] Robin Emmot: “Europe plan undersea cable to skirt U.S. spying”, en *Reuters* (24 de febrero de 2014), en: http://www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224.

[24] Ewen MacAskill; Julian Borger; Nick Hopkins; Nick Davies y James Ball: “GCHQ taps fibre-optic cables for secret access to world’s communications”, en *The Guardian* (21 de junio de 2013), en: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa