

## Resumen

Cuando se empezó a rumorear la existencia de Echelon, sistema que parecía sacado de las novelas de Ian Fleming, pocos profesionales informáticos hubieran apostado por su existencia real. Con el reconocimiento oficial de su existencia por parte del propio Parlamento<sup>1</sup> a partir de bastantes pruebas acumuladas, la idea ha cambiado... hacia cómo defenderse de ese nuevo Gran Hermano. No es propósito del presente artículo juzgar la necesidad de los estados a la vigilancia de sus ciudadanos o ciudadanos de otras naciones, sino simplemente dar en unas breves pinceladas noticia de estas nuevas formas de control. Echelon, Enfpol, Carnivore y algún sistema que aparecerá en un futuro a corto plazo quizá modifiquen nuestros hábitos de navegación por internet.

Juan Vte. Oltra Gutiérrez – Universidad Politécnica de Valencia. [jvoltra@omp.upv.es](mailto:jvoltra@omp.upv.es)

## Palabras Clave

Echelon, Carnivore, Enfpol, Criptografía

### 1. *Echelon hoy*

Puede parecer un poco chocante presentar a Echelon en sociedad, pero no está de más de cara a establecer ciertos elementos básicos de partida.

Tomando como propia la definición que hace Claudio Hernandez<sup>2</sup>, entendemos como tal el *Sistema de satélites norteamericanos que permiten “espíar” al usuario de a pie. El sistema Echelon permite interceptar comunicaciones de teléfono, radio o de Internet. Los satélites de Echelon no son los únicos elementos de este sistema de espionaje, además de ellos, podemos encontrarnos con sistemas “capturadores” de señales de radio, Escaneres y sistemas informáticos.*

Podría pensarse por parte de alguien que no fuera seguidor de la prensa especializada que el autor citado exagera o que ha sufrido una sobredosis de novelas de ciencia ficción y que está próximo a convertirse en un quijote cybernético. No es el caso y para dar peso a una definición tan contundente acudamos a una fuente con solvencia y de la que al menos en principio, la seriedad se le supone: el Parlamento europeo. En el “PROYECTO DE INFORME sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON)” de 18 de mayo de 2001<sup>3</sup>, podemos leer: (página 12)

"(...) No hay ninguna razón para seguir dudando de la existencia de un sistema de interceptación de las comunicaciones a nivel mundial en el que participan los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda en el marco del Acuerdo UKUSA; considerando, asimismo, que según las informaciones de que se dispone, es probable que su nombre sea realmente "ECHELON", si bien no es éste un aspecto de importancia primordial (...) El sistema no se utiliza para interceptar comunicaciones militares, sino privadas y económicas (...)"

Un tema que no es precisamente nuevo para nuestros europarlamentarios. Ya en septiembre de 1998, en un resumen preparado como documento de base para el periodo parcial de sesiones, titulado “EVALUACIÓN DE LAS TECNOLOGÍAS DE CONTROL POLÍTICO”<sup>4</sup> podíamos leer:

---

<sup>1</sup> 'Echelon lee los correos electrónicos, advierte la UE' (El Mundo, 30.5.2001)

<sup>2</sup> **Hernández, Claudio. Hackers. Los piratas del Chip y de Internet.** Disponible online en <http://www.webshack-it.com/kriptopolis/hackers.zip>

<sup>3</sup> Disponible en: [http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon\\_es.pdf](http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_es.pdf)

<sup>4</sup> Disponible en: [http://www.europarl.eu.int/stoa/publi/166499/execsum\\_es.htm](http://www.europarl.eu.int/stoa/publi/166499/execsum_es.htm)

"(...) El sistema [*Echelon*] fue descubierto por primera vez en la década de los 70 por un grupo de investigadores del Reino Unido (Campbell, 1981). (...) Forma parte del sistema UK/USA, pero a diferencia de muchos de los sistemas electrónicos de espionaje desarrollados durante la guerra fría, ECHELON está diseñado para objetivos fundamentalmente no militares: gobiernos, organizaciones y empresas en prácticamente todos los países. El sistema ECHELON funciona interceptando de forma indiscriminada enormes cantidades de comunicaciones, seleccionando posteriormente lo que es de valor mediante el uso de ayudas de inteligencia artificial (...) para encontrar palabras clave.

*"(...) Aunque no más de la mitad de estas acusaciones fuesen ciertas, el Parlamento Europeo debería actuar para garantizar que estos potentes sistemas de vigilancia funcionen dentro de un consenso más democrático, ahora que la guerra fría ha terminado. Está claro que las políticas internacionales de los Estados miembros de la Unión Europea no siempre son congruentes con las de los Estados Unidos, y, en términos comerciales, el espionaje es el espionaje. Ninguna autoridad de los Estados Unidos permitiría que una red de espionaje similar de la UE funcionase en su territorio sin estrictas limitaciones, en caso de permitirla. Tras un completo examen de las repercusiones de las operaciones de estas redes, se recomienda al Parlamento Europeo que establezca un adecuado control independiente y procedimientos de supervisión, y que se impida cualquier esfuerzo de ilegalizar la codificación por parte de cualquier ciudadano de la UE, salvo que se hayan creado estos sistemas de control y responsabilidad democráticos."*

Escalofriante, aun viendo que aparecen como título las palabras "Proyecto de informe", por lo que pueden quedar dudas sobre su correspondencia con la realidad. Pero desde el 3 de julio de 2001 Echelon existe de forma oficial. Esa fue la fecha en la que la comisión de Investigación del Parlamento Europeo despejó cualquier posible duda sobre su existencia.

## **2. ¿Quién está en peligro?**

De acuerdo al citado proyecto de informe, Echelon, por sus mecanismos de interceptación, recoge un "*porcentaje muy limitado*" de las comunicaciones, pudiendo por otra parte, "*interpretar una proporción muy escasa*" de éstas. No perdamos de vista que esto sucede por limitaciones técnicas, no políticas, estratégicas ni éticas. Se trata sin duda de algo que va más allá de la ética, de la privacidad de datos o del hacking "casero" (netbus o back orifice<sup>5</sup>). Podríamos asimilarlo a un Phreaking<sup>6</sup> del más alto nivel, que prescinde de ética y ley, como es común cuando se trata de actos de espionaje.

Esto nos debe impedir olvidar que, aunque se trate de un alcance limitado, no implica que el peligro sea reducido. De nuevo, el euro parlamento nos recuerda que "*los posibles peligros que un sistema como ECHELON encierra para la esfera privada y la economía no sólo se derivan del hecho de que se trate de un sistema de interceptación especialmente poderoso; más bien se deriva de que este sistema funciona en un ámbito carente, casi por completo, de regulación jurídica (...) La persona objeto de observación, por ser extranjera para el país observador, no dispone*

---

<sup>5</sup> Estos términos corresponden a lo que se ha dado en llamar "Caballos de Troya". Se trata de programas que aparentan tener una utilidad mientras en realidad hacen otras cosas (por lo general perniciosas) o bien aplicaciones que permanecen ocultas al propietario del ordenador mientras realizan actuaciones sobre el mismo. Generalmente son instalados en computadoras ajenas para que el hacker que lo instaló pueda desde obtener información sobre lo que ocurre en el sistema o incluso realizar operaciones desde esta.

<sup>6</sup> Se entiende por phreak el uso del teléfono, o de las redes y servicios telefónicos, gratis o con un coste menor del normal. Por extensión, también se conoce así a la intervención de líneas telefónicas o al tratar de entrar a cualquier red rompiendo sus sistemas de seguridad.

de ninguna clase de protección jurídica intraestatal. Por ello, **cada persona** (el subrayado es nuestro) *está en situación de completa indefensión frente a este sistema.*"

No nos encontrábamos por tanto ante el dilema de legalidad o ilegalidad, sino en medio de la más absoluta alegalidad. Y lo que resulta más preocupante, no hay que cubrir un solo frente: Echelon ha producido un efecto dominó que ha llevado a que Europa promueva su Enfopol<sup>7</sup> y a que Rusia anuncie su propio sistema de espionaje, primo hermano del USUKA.

Es más: cuando se habla de **cada persona** no se incurre en un alarmismo. No importa si se ocupa o no un cargo o donde se esté en la escala social: Echelon vigila a todo el mundo, desde Diana, Princesa de Gales<sup>8</sup> hasta los mensajes que el Papa mandó a la Madre Teresa de Calcuta, pasando por ciudadanos de a pie, como reveló el programa "60 Minutos" de la cadena americana de TV CBS. El programa relató el caso de una mujer cuyo nombre y número de teléfono terminaron en la base de datos de Echelon como una posible terrorista después de que mantuvo una conversación con una amiga a la que le contó que su hijo hizo un papel durante una obra de teatro en el colegio, usando la expresión "*he bombed*" (en inglés "*puso una bomba*", pero también en sentido figurado puede ser "*fue muy deprisa*"). El sistema detectó la conversación y el analista de Echelon, que no estaba muy seguro de qué estaban hablando, incluyó a la mujer.

### **3. Que hacer**

Aquí tendríamos que presentar dos planos: empresas y ciudadanos. Las empresas ya han sufrido muchos ataques de espionaje industrial por medio de Echelon (recordemos los 6000 millones de dólares que el consorcio aeronáutico europeo Airbus perdió frente a la Mc Donnell Douglas o al robo de procedimientos que sufrió la compañía BASF). En cuanto a las formas de protección: jurídica, como es obvio, el robo de secretos de empresa es ilegal, aunque las penas que se aplican son siempre inferiores a los casos de espionaje militar. En el caso de los Estados Unidos de América, las leyes prohíben las actividades de espionaje de las empresas industriales entre sí, no quedando bien definido si la ley limita también la actividad de espionaje industrial de todos los servicios de inteligencia. ¿Qué ocurre cuando éstos facilitan a las empresas las informaciones obtenidas mediante espionaje?. Tengamos en cuenta que este tipo de escuchas no deja rastros ni pruebas admisibles en los tribunales, lo que complica más la situación.

Ante este aparente páramo legal, se impone una "autodefensa" técnica, tanto para las empresas como para los particulares. El comercio electrónico y las transacciones bancarias electrónicas dependen de que las comunicaciones por internet sean, o al menos aparenten serlo, seguras. Si no se pueden garantizar unas comunicaciones seguras, las empresas orientadas hacia estos mercados estarán condenadas al fracaso, pues sus clientes potenciales perderían la confianza que tienen. Esta es la dirección hacia la que parece apuntar la UE con el citado Informe en sus siguientes puntos:<sup>9</sup>

---

<sup>7</sup> El 7 de Mayo de 1999, el Parlamento Europeo aprobó la Resolución del Consejo sobre interceptación legal de las comunicaciones, conocida como Resolución Enfopol. Se abre así el camino a un sistema de interceptación y vigilancia de las comunicaciones en todo el territorio de la Unión Europea.

<sup>8</sup> Esta información, referente al espionaje de la Princesa de Gales y al del Papa Juan Pablo II, aparecieron en la edición del 27 de febrero de 2000 del Sunday Times. Disponible en: <http://www.sunday-times.co.uk/>

<sup>9</sup> PROYECTO DE INFORME sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas Páginas 18 y 19.

"15. Se insta a la Comisión y a los Estados miembros a que desarrollen programas que aumenten el grado de concienciación de los ciudadanos y de las empresas en relación con los problemas relacionados con la seguridad y, al mismo tiempo, a que brinden asistencia práctica para la concepción y la aplicación de sistemas de protección de carácter mundial;

"16. Se solicita a la Comisión y a los Estados miembros que adopten medidas adecuadas para impulsar, desarrollar y producir tecnologías y software europeos de **cifrado**, así como, en particular, que apoyen proyectos que tengan como objetivo el desarrollo de software de encriptación de utilización sencilla y cuyo código fuente sea público;

"17. Se insta a la Comisión y a los Estados miembros a que impulsen proyectos de software cuyo texto de base sea público, ya que este es el único modo de garantizar que no se incluirán "backdoors" ("open-source software");

"18. Se insta a las instituciones europeas y a las administraciones públicas de los Estados miembros a que **cifren** el correo electrónico sistemáticamente para que, a largo plazo, se convierta en una norma ..."

El Parlamento Europeo promueve así la defensa contra Echelon y otros sistemas de espionaje con una técnica clara y bien conocida: el cifrado.

Aquí deberíamos hablar de Phil Zimmerman y de Pretty Good Privacy (PGP), así como de herramientas similares de cifrado personal como GnuPG, S/MIME... Pero no parece necesario extenderse más en esta posibilidad de protección, dada la amplia variedad de sitios internet donde se puede encontrar desde productos hasta manuales. La revista Kriptópolis incluso ofrece un "curso acelerado" de una hora, cuya visita recomendamos<sup>10</sup>.

Si en lugar de alarmarnos por la posibilidad de que seamos sujetos de un seguimiento empleásemos cifrado en nuestras comunicaciones, tomaríamos parte activa en la oposición a este nuevo "Gran Hermano". Pero existen colectivos que van más lejos, basándose en el adagio que dice que la mejor defensa es un buen ataque, como el que se dio en el "Jam-Echelon", el pasado 21 de octubre del 2000. Tras un amplio acuerdo de convocatoria común, empezaron a circular miles de mensajes llenos de palabras como "bomba", "atentado", "presidente" o "explosivo" y sus variantes en distintos idiomas. El propósito de esta acción coordinada no era otro que el de saturar Echelon con un exceso de información. Es imposible evaluar el efecto que esto pudo tener sobre Echelon, pues no podemos afirmar que conozcamos a la perfección su *modus operandi*. Pero este acto de protesta marcó un antes y un después en lo que se refiere a la conciencia pública de la existencia de Echelon y sus repercusiones en la libertad de los individuos. A partir de ese momento, muchos internautas empezaron a insertar como firma de sus mensajes un texto en inglés parecido al siguiente:

---

---

*Explosives, guns, assassination, conspiracy, primers, detonators,  
grenades, rockets, president*

---

*Dear Echelon Team:*

*We're aware that this message could contain some of your favourite key words and probably you'll be scanning this very soon. We do hope that this unbearable situation doesn't last much more but in the meantime and just in case we want to cry: 'God bless Mr. Bush!' ;-)*

---

<sup>10</sup> <http://www.kriptopolis.com/pgp/index.html>

En otras palabras, se pasó de la duda sobre si Echelon era real o no, a la preocupación por hacer algo sobre ello.

#### **4. Lo que viene**

Hace un tiempo, los funcionarios del gobierno de EE.UU. empleaban una anécdota para explicar por qué mantenían unos controles tan estrictos en sus políticas de exportación de software para cifrado. Contaban que los investigadores que resolvieron el caso de las bombas que explotaron en el World Trade Center de Nueva York pudieron encontrar evidencias en el ordenador del terrorista porque utilizó cifrado de bajo nivel. Si hubiera utilizado un cifrado más potente (entonces restringido) hubiera sido imposible obtener pruebas para condenarlo.

Esta historia u otras similares podrían ser "desenterradas" por el FBI para defender su programa Carnivore (o DCS1000, como ha sido rebautizado en busca de una mejor prensa). Éste intercepta mensajes de correo electrónico y otras informaciones transmitidas a través de redes informáticas. El FBI<sup>11</sup> ha descrito a Carnivore como una herramienta de vigilancia electrónica, que sólo será usada de manera restringida y después de una autorización explícita dada por el Departamento de Justicia.

Aun es pronto para saber el funcionamiento y los resultados de Carnivore: al igual que en los primeros momentos con Echelon, solo podemos especular sobre lo que el FBI está haciendo con este programa, pero los antecedentes generan bastante preocupación sobre abusos de poder. La alarma no es en balde, pero debemos recordar las muchas etapas que los funcionarios gubernamentales del FBI tienen que cumplir para utilizar Carnivore: por una parte, el fiscal debe obtener la aprobación de un funcionario de alto nivel del Departamento de Justicia, y por otra, las solicitudes para la vigilancia electrónica también deben demostrar la "causa probable" para sospechar que se está realizando una actividad ilegal, así como especificar los delitos que se estarían cometiendo, los nombres de las personas involucradas y el proveedor de servicio de Internet (ISP) que está utilizando el sujeto. Además, el empleo de Carnivore ha de concentrarse en obtener evidencia específica, no información al azar, aunque analiza un montón de paquetes digitales, incluyendo el correo electrónico de personas que no tienen nada que ver con la investigación.

Carnivore no es tan sólo un problema para los ciudadanos de EE.UU. El pasado 3 de diciembre, el diario británico *The Observer*<sup>12</sup> hablaba de un nuevo plan para espiar todas las comunicaciones británicas. La noticia se basa en un documento del NCIS, *National Criminal Intelligence Service* del gobierno británico,<sup>13</sup> dirigido a la Asociación de Jefes de Policía, el Servicio de Aduanas, el Servicio de Seguridad, el Servicio Secreto de Inteligencia ... y el GCHQ, encargado del espionaje electrónico en el Reino Unido, donde se considera que deben almacenarse los datos relativos a las comunicaciones por un período de tiempo de hasta siete años. No se guarda el contenido de las comunicaciones en sí, sino lo que se llaman "datos asociados a la llamada": números de destinatario y remitente, tipo de red usada, datos relativos al cobro de llamada... haciendo un símil, resultaría como si nuestro cartero fotocopiase los sobres que recibimos antes de darnoslos.

En el caso del Reino Unido, Carnivore almacenaría los datos cuyo origen o punto de llegada sean el Reino Unido, incluso si es solamente un punto de paso de dichos datos. Es decir, una comunicación entre Alemania y México que pase por el Reino Unido podrá ser "almacenada".

Quizá sea el momento de empezar a pensar en la entrada en acción de otro Carnivore europeo (y de paso, replantearnos seriamente nuestros hábitos de navegación) si nos

---

<sup>11</sup> <http://www.fbi.gov/hq/lab/carnivore/carnivore.htm>

<sup>12</sup> [http://www.observer.co.uk/uk\\_news/story/0,6903,406191,00.html](http://www.observer.co.uk/uk_news/story/0,6903,406191,00.html)

<sup>13</sup> el documento *filtrado* está disponible en <http://cryptome.org/ncis-carnivore.htm>.

fijamos que el Consejo de Ministros Europeo (es decir su órgano ejecutivo) ha publicado un nuevo borrador<sup>14</sup> de su tratado de cibercriminación, dónde se han incluido dos nuevas secciones sobre la interceptación de las comunicaciones y dónde podemos leer que todos los proveedores de servicio deben bien dirigir técnicamente la vigilancia cuando se les solicite, o bien asistir técnicamente a las fuerzas de la ley.

### *¿final?*

El artículo precedente fue escrito mucho antes de los tristes sucesos del 11 de septiembre. Nadie podía esperar un atentado de la magnitud del que destruyó un ala del pentágono y las torres del World Trade Center (por mucho que algunos, precisamente vía internet, se empeñen en adjudicarle esa visión a Nostradamus).

Pero esos aviones se llevaron por delante, o al menos transformaron, otras cosas. Por ejemplo, la tendencia de la CIA (e imaginamos que otras agencias de investigación) a prescindir de buena parte del elemento humano en su trabajo para confiar de manera –ahora lo vemos- excesiva en la tecnología.

Echelon, Carnivore... no fueron capaces de detectar (o al menos así se nos ha asegurado desde el gobierno USA) los preparativos de este atentado múltiple. Cuchillos que hacen inútiles satélites, como en una mala película futurista, se nos decía desde la CNN.

Sin embargo, a pesar de su fracaso a priori, pudimos comprobar como empresas como Hotmail o AOL pusieron todo su poder al servicio de este “filtrado institucional”. Todo mensaje enviado los días siguientes era examinado y, aquellos que fueran escritos en árabe, estudiados con especial detenimiento. Cualquiera que emplease los grupos de distribución de Yahoo pudo comprobar como sus envíos se demoraban un mínimo de 3 horas en la semana siguiente al atentado. Casi se podía notar la respiración del Gran Hermano en nuestro cuello.

Y, a todo esto, poca o ninguna protesta por parte de los internautas más combativos. Quizá empiezan Echelon y Carnivore a ser vistos de otra manera . El mejor indicio de ello es que tras los ataques terroristas del 11 de septiembre, el Senado americano empezó a revisar la legislación para facilitar la vigilancia del tráfico del correo electrónico y otras comunicaciones electrónicas, por medio de una reforma que presentó el senador Orrin Hatch, la cual simplificará el camino de los investigadores para conseguir una orden judicial para interceptar comunicaciones electrónicas.

De todas formas, cabe hacer una reflexión final: posiblemente Echelon fuera ineficaz en esta ocasión por el empleo de cifrado por parte de los terroristas o porque también usaron para sus órdenes medios menos sofisticados como visitas, etc. (las huellas de sus preparativos si parece que ha podido seguirse por la red). Pero en cualquier caso,... esto quiere decir que, mientras los culpables no son controlados, millones de cuentas de ciudadanos inocentes han sido estudiadas con detalle.

¿Debe cambiar nuestra visión sobre Echelon después de lo que hemos visto o vivido?. Particularmente, apuesto por el NO como respuesta... y el Parlamento Europeo tampoco parece que justificará ahora lo que antes criticaba.

---

<sup>14</sup> <http://conventions.coe.int/treaty/EN/projets/projets.htm>