Red Echelón "un problema bioético mundial [Red Echelon "a global bioethical problem"]

RED ECHELON
" UN PROBLEMA BIOÉTICO MUNDIAL"

Jairo E. Márquez D.

La red Echelon (escalón) conocida como la gran oreja, es un sistema informático robusto que vigila simultáneamente todas las comunicaciones, y está soportado en un conjunto de estaciones de escucha, radares y satélites, apoyada por una flota de aviones espía y submarinos enlazados a través de bases terrestres dispersas por todo el planeta Tierra. Su objetivo es espiar las comunicaciones mundiales (correos electrónicos, fax, comunicación por cable, satélite, etc), con el fin de luchar contra el terrorismo, tráfico de drogas y en general todo lo que atente contra la nacionalidad de Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva zelanda.

La red Echelon (escalón) o conocida también como la Gran Oreja, se perfiló en la primera guerra mundial, plasmándose en realidad en la segunda Guerra mundial, donde Estados Unidos y Gran Bretaña crearon un sistema de espionaje e intercambio de información denominado **UKUSA (UK = United Kingdom and USA = United States of America)**, cuya finalidad era la de interceptar comunicaciones del bloque del Pacto de Varsovia y China. Posteriormente se anexaron los países de Canadá, Australia y Nueva Zelanda.

Inicialmente estados unidos estableció la alianza denominada ***SIGINT***, en una reunión celebrada en agosto de 1940 entre estadounidenses y británicos, de esta época en adelante se creó una cooperación entre estos dos países en lo concerniente al criptoanálisis, descifrado de mensajes e inteligencia.

Tras la guerra Gran Bretaña dio el primer paso para continuar con la Alianza SIGINT. Las bases se acordaron en una gira mundial realizada en 1945 por miembros británicos de inteligencia. Uno de los objetivos era enviar personal europeo al Pacífico para la guerra con el Japón. En este contexto, se acordó con el gobierno de Australia poner recursos y personal (británicos) a disposición de los servicios de inteligencia australianos, al final de este proceso fueron contactados los países de Nueva zelanda y Canadá.

En 1945 el presidente Truman firmó un memorándum confidencial, el cual fue pieza clave para la consolidación de la Alianza SIGINT en tiempos de paz. Entre los años de 1946 y 1948 se efectuaron una serie de reuniones confidenciales con fines de establecer el norte de esta alianza, terminando en un texto definitivo llamado Acuerdo UKUSA en junio de 1948.

Echelon entró en operación al cien por ciento en el año de 1977, cuando la tecnología electrónica de los satélites y estaciones de escucha espías dejaron de ser incipientes, permitiendo la interceptación de comunicaciones de la redes satelitales llamadas **INMARSAT** (Interim International Maritime Satellite) que actualmente presta servicios de comunicación móvil área, marítima y terrestre con sus nueve satélites no polares. **INTELSAT** (Organización Internacional de Telecomunicaciones por Satélite), se fundó en 1964, y está conformada por consorcio de 144 gobiernos que presta servicios a 200 países de telefonía, actualmente la flota de satélites es de 25 que cubren prácticamente todo el globo terráqueo. Se privatizó en el año 2001.

Actualmente todos los sistemas de satélites mundiales están siendo espiados por esta red a parte de los ya nombrados como son:

Sistema **INTERSPUTNIK** fue fundada en 1971 por nueve países como una agencia de la antigua Unión Soviética, con una misión similar a la de INTELSAT. Su flota de 4 satélites geoestacionarios cubren todo el globo. Cuenta con 24 estados miembros y 40 países como usuarios;

Sistema **PANAMSAT**, se fundó en 1998 como proveedor de un sistema global de satélites. Cuenta con una flota de 21 satélites que prestan servicios de televisión, Internet y telecomunicaciones en todo el mundo. Su cobertura está centrada en los Estados Unidos.

Sistema **EUTELSAT**, pertenece a la Agencia Europea con 40 países miembros. Consta de 18 satélites que cubren la Tierra excepto las órbitas polares.

Sistema **HISPASAT**, cubre la zona de los países de Portugal y España con conexión a las dos Américas

Sistema **TELECOM**, satélite francés que conecta a Francia, África y Sudamérica.

Sistema **ITALSAT**, explota los satélites de telecomunicaciones que cubre Italia y países contiguos, luego la recepción solo es posible en Italia.

Sistema **ARABSAT**, similar a Eutelsat en la zona árabe y se fundó en 1976. la integran 21 países árabes. Los satélites se utilizan para transmisión de servicios de televisión como para las telecomunicaciones.

Sistema **PALAPA**, funciona desde 1995 y es similar a Arabsat. Es un sistema Indonesio que cubre la zona del Asia meridional.

Sistema **AMOS**, satélite israelí cuya huella cubre el Oriente.

¿CÓMO FUNCIONA LA RED ECHELON?

El sistema de espionaje está basado en la escucha de las comunicaciones por medio de sniffers y su posterior filtrado. Este filtrado se centra en la identificación de palabras clave previamente fijadas en grandes bases de datos llamados "diccionarios". Estas palabras pueden pertenecer tanto a textos como a voces reales y ser pronunciadas y/o escritas en varios idiomas (inglés, español, francés, árabe, chino, japonés, etc). El sistema informático posee programas de recono-

cimiento de voz basados en inteligencia artificial. Se habla que puede filtrar 2.000 millones de mensajes en una hora. Tal y como está organizada la red, ésta no permite, por ejemplo, a las autoridades Neozelandesas o Canadienses conocer los diccionarios usados por la **NSA** en Los Estados Unidos y la **GCHQ** de Gran Bretaña, si bien lo contrario sí es posible.

Cave anotar que todo informe va con copia a la NSA, los servicios británicos reciben las comunicaciones en Westmister- Londres, que son procesadas por un supercomputador que posee su propio diccionario que traduce la información diferentes idiomas según el caso.

Los sistemas de los supercomputadores de rastreo de la NSA están denominados con nombres clave. Así: si es de conversación se le denomina ORATORY. El nombre del procedimiento de las escuchas telefónicas es MANTIS y el de los fax MARYFLY. El tráfico de Internet se intercepta a través de las llamadas "capas de Transporte"; se definen palabras clave, por ejemplo, Busch, atentado, narcotráfico, Sadam Hussein, Castro, siempre definidas en varios idiomas. Se pasa entonces a rastrear las comunicaciones mundiales. Se habla de un poder de captación del 90% de las mismas, si bien se cree que este porcentaje solo afecta a las comunicaciones de Internet. Teniendo en cuenta que casi todas las comunicaciones vía Internet mundiales, independientemente de dónde se produzcan, pasan por nodos de comunicación de los Estados Unidos y por nueve puntos de control de la NSA (National Security Agency, Agencia de Seguridad Nacional de los Estados Unidos). Dos de ellos están directamente controlados por la Administración norteamericana: College Park, en Maryland, y Sugar Grove (Virginia) y un sistema de apoyo en Mountain View (California). Los principales centros de intercepción y rastreo de comunicaciones de Echelon se encuentran situados en Menwith Hill (Gran Bretaña), Bad Aibling (base militar Norteamérica en Alemania), Sabana Seca (Puerto Rico), Leitrim (Canadá), Shoal Bay (Australia) y Waihopai (Nueva Zelanda). La capacidad de captación de estas estaciones de radiocomunicaciones se incrementa constantemente. La base de Sugar Grove, situada en una remota área de las montañas Shenandoah, a unas 250 millas al suroeste de Washington, se hallan dispuestas una serie de

antenas satelitales las cuales están orientadas al espacio para interceptar comunicaciones europeas y atlánticas.

La estación de escucha de ***Morwenstow*** (Reino Unido) se encarga de la coordinación de las diferentes escuchas realizadas a los satélites Intelsat de Europa, océano Atlántico y océano Pacífico.

Las estaciones de ***Menwith Hill*** (Gran Bretaña) y ***Bad Aibling*** (Alemania) se encargan de lo mismo, pero de los satélites que no forman parte de la red Intelsat (como los Inmarsat).

También se sabe de la existencia de un submarino llamado USS Patch (parche) encargado de intervenir (pinchar) las comunicaciones por cable submarino.

Alrededor de los siete nodos fuera de los Estados Unidos se apoyan el resto de las computadoras terrestres, satélites, submarinos y aviones formando una gran red que cubre todo el planeta. También se sitúa el núcleo central del programa informático en la estación antes mencionada de Menwith Hill.

Una vez que se detecta una comunicación conteniendo o bien palabras clave o bien ciertas combinaciones de ellas (por ejemplo, "bomba", "gobierno" y "atentado" en el mismo mensaje), el sistema informático pasa a monitorearla y posteriormente grabarla. Esta comunicación será entonces etiquetada y enviada a distintos centros de análisis. Dependiendo del origen y fecha de la comunicación será marcada con un número clave. Se transcribe, descifra, traduce y se guarda como un informe; los cuales reciben un código dependiendo del grado de seguridad otorgado al mismo: "Morai" equivale a secreto. Después le siguen los códigos "Spoke" (más secreto), "Umbra"(alto secreto), "Gamma" (comunicaciones rusas) o "Druid" (destinado a países no miembros de la red).

Después se asigna un código más relacionado con cada una de las agencias de seguridad, dependiendo cual sea, será reenviado el informe a través del sistema central de la red UKUSA, denominado "Platform".

Código	Agencia	País
Alpha	GCHQ	Gran Bretaña
Echo	DSD	Australia
India	GCSB	Nueva Zelanda
Uniform	CSE	Canadá
Oscar	NSA	Estados Unidos

Código asignado, enlace a la agencia de seguridad y país al que pertenecen

Las siglas equivalen a:

- **NSA** (USA): National Security Agency.
- **GCHG** (UNITED KINGDOM): Govenrment Communications Headquarter.
- **CSE** (CANADÁ): Communications Security stablishment
- **DSD** (AUSTRALIA): Defense Signals Directorate
- **GCSB** (NEW ZELAND): Government Security Bureau

Algunas palabras clave que el diccionario de Echelon toma como subversivos y que atenten contra la seguridad nacional de los países miembros son:

Enfopol, Gadafi, V.O.A, uranio, plutonio, RAN, Kennedy, NATO, ETA, F80, submarino, Antártida, megatones, subversivo, Serra, Dzokhar Dudayev, unabomber, UKUSA, NSA, FBI, CIA, NASA, hacker, Pekin, Mao, heroina, Bill Gates, DEA, Ginebra, Chechenia, Ami Ayalom, Bruselas, Yelsin, mafia, Jeff O'Connor, M.A.F.I.A.,HB, Pervez Musharraf, talibán, Romano Prodi, afgano, Barry McCaffrey, Nawaz Sharif, Atal Behari Vajpayee, Jaswant Singh, Ved Prakash Malik, Wiranto, Yusuf Habibie, General, portaviones, Hamás, Shin Beth, OLP, antiaerea, Bill Clinton, TPCPN, Jesse Helms, Trent Lott, Abu Jamal, AFL-CIO, Ernesto Zedillo, cartel, PRI, Pinochet, Rosso José Serrano, Vaticano, Helmer Villafanía, Janet Reno, Bruselas,Yihad Islámica, Comisión Europea, Ehud Bark, Oscar SS-N-27, Tampere, UE, euro, Yasir Arafat, Yuri Scurátov, Microsoft, General Videla, Fidel Castro, cañón magnético,Bush,Yabrán, DEA, ENL, FARCS, nazi, judio, CONDOR, Bush, ALACRAN, STOA, Comunista, izquierda, EVA, Galtieri, Malvinas, Falkland, Pucará, secret, war, Yugoslavia,

Contras, Ormart, SIDE, CESID, MOSSAD, MI5, MI6, Echelon, Carníve, seprin, Al Kssar, IRA, Gladio, Gladietor, kgb, Rusia, Tripóli, saddam, housein, AMIA, nsakey, white house, gov, FA117, Phanton F15, De la RUA, George W. Bush, Choripan, armas, army, US AIR FORCE, US Navy, US, Hezbola, peronismo, radiocalismo, kurdo, KKK, etc.

Si se considera que es una transmisión peligrosa para los intereses de los estados que componen la red Echelon los participantes de esa comunicación pasarán a formar parte de una lista negra y sus comunicaciones y acciones serán espiadas a partir entonces en mayor o menor medida, dependiendo de distintas consideraciones que los responsables crean oportunas. Los responsables de la red asumen que se van a tomar como peligrosas comunicaciones que en realidad no lo son debido al factor error, y la persona que ha transmitido ese mensaje será "injustamente" catalogada como peligrosa, pero asumen esas situaciones como normales e insignificantes.

¿CUÁLES SON SUS COMPONENTES?

Sobre los medios de que disponen las agencias implicadas poco se puede decir salvo que están perfectamente capacitadas para realizar tales acciones. La NSA tiene un presupuesto anual de varios miles de millones de dólares y mantiene bajo su control 120 satélites militares para monitorizar las líneas de comunicación mundiales. Sus antenas de recepción cubren la totalidad del planeta. Ejemplos de satélites militares son:

MILSTAR: Programa de los Estados Unidos que gestiona 6 satélites geo-estacionarios para la intercomunicación de sus tropas a nivel mundial (bases terrestres, navíos, aviones,...).

DSCS: 5 satélites que permiten una comunicación global. También de los Estados Unidos.

SKUNET: Sistema británico con cobertura mundial.

Los sistemas Syracuse (francés) y Sicral (italiano) viajan de manera furtiva entre los satélites civiles (Telecom, Hispasat e Italsat) y utilizan la banda X para la recepción y transmisión de señales, su alcance es regional.

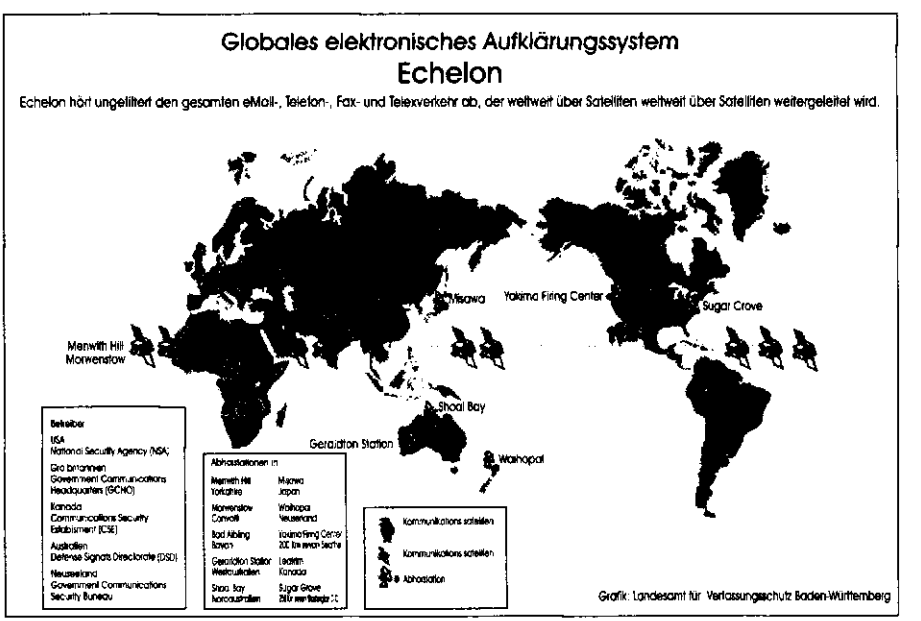
Los militares rusos utilizarían también el canal X de los satélites MOLNYIA.

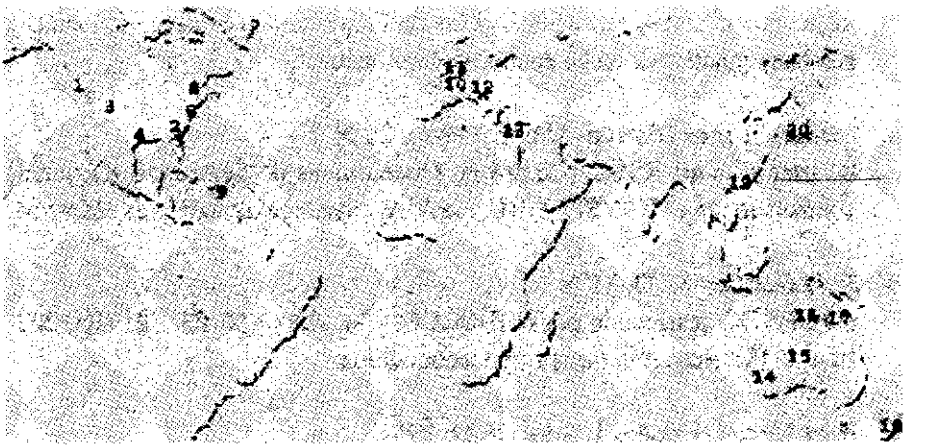
La OTAN tiene sus propios satélites como son: NATO IIID, NATO IVA y NATO IVB.

SKYNET (Británico)

En Menwith Hill. VORTEX, MAGNUM y ORION.

Las cifras relacionadas con la composición de esta red es extrema. Hay que tener en cuenta además que se trata de una estructura de carácter secreto, por lo que no existen datos oficiales al respecto. Pero se conocen las ubicaciones de algunas de las estaciones de escucha dispersas por todo el planeta, según se observa en la siguiente gráfica.





Lista de estaciones de escucha y localización geográfica.

1. ***Yakima*** (Estados Unidos) 120°O, 46°N
   Base del 544° Grupo de Inteligencia (Destacamento 4) de la Air Inteligence Agency (AIA) y del Naval Security Group (NAVSECGRU). Tiene 6 antenas de gran diámetro satelitales orientadas hacia el sistema Intelsat del Pacífico y Atlántico. Una de las antenas estaría orientada hacia el satélite Immarsat 2. Se encarga del «Intelligence Support» (apoyo informativo) respecto a la escucha de satélites de comunicación a través de estaciones de la Marina (de Estados Unidos).

2. ***Sugar Grove*** (Estados Unidos) 80°O, 39°N
   También en esta base se encuentra el NAVSECGRU y el 544° Grupo de la AIA (Destacamento 3). Cuenta con 10 antenas satelitales de rastreo de gran envergadura (aproximadamente 18 metros).

3. ***Buckley Field*** (Estados Unidos) 104°O, 40°N
   Dirigida por el 544° IG (destacamento 45). Constaría de al menos 6 antenas de las cuales cuatro superan los 20 metros. Oficialmente su cometido consiste en la recopilación de datos sobre acontecimientos en el ámbito

nuclear mediante satélites SIGINT (satélites que captan e interpretan señales electromagnéticas), en su análisis y evaluación.

4. ***Medina Annex*** (Estados Unidos) 98°O, 29°N
   Se trata de otro RSOC (Centro de Operaciones de Seguridad Regional) controlado por el NAVSECGRU y la AIA, cuya área de acción es el Caribe.

5. ***Fort Gordon*** 81°O, 31°N
   Otro RSOC gestionado por el INSCOM y la AIA (702° IG, 721° IG, 202° IB, 31° IS). Sus cometidos son desconocidos.

6. ***Fort Meade*** (Estados Unidos)76°O, 39°N
   Es la sede de la NSA (Agencia de Seguridad Nacional de los Estados Unidos).

7. ***Kunia*** (Hawai, Estados Unidos) 158°O, 21°N
   Gestionada por el NAVSECGRU, el RU y la AIA. Oficialmente es un Centro de Operaciones de Seguridad Regional (RSOC) y tendría como tareas asignadas la preparación de información y comunicaciones así como el apoyo criptográfico. La verdad es que sus funciones específicas no son claras.

8. ***Leitrim*** (Canadá) 75°O, 45°N
   Forma parte de un intercambio de unidades entre Estados Unidos y Canadá. Consta de 4 antenas, dos de ellas tienen diámetros de 12 metros. Oficialmente esta estación se dedica a la «calificación criptográfica» y a la interceptación de comunicaciones diplomáticas.

9. ***Sabana Seca*** (Puerto Rico) 66°O, 18°N
   Utilizada por el Destacamento 2 del 544° AIA y por el NAVSECGRU. Cuenta con varias antenas, una de ellas de 32 metros. Procesa las comunicaciones por satélite, brinda servicios de criptografía y comunicación y sirve de apoyo a labores realizadas por la Marina y por el Ministerio de Defensa, como por ejemplo recoger información proveniente del sistema satelital COMSAT.

10. ***Morwenstow*** (Inglaterra) 4° O, 51°N
Estación manejada por el GCHQ (Servicio de Inteligencia británico). Cuenta con unas 21 antenas, tres de ellas de 30 metros. No se conoce su cometido especial, pero por su configuración y localización geográfica todo indica que se dedica a la interceptación de comunicaciones por satélite.

11. ***Menwith Hill*** (Inglaterra) 2°O, 53°N
Utilizada conjuntamente por Estados Unidos y Gran Bretaña. Por parte de los primeros, se encuentran en la estación el NAVSECGRU, la AIA (45°IOS) y el ISNCOM. La estación pertenece al Ministerio de Defensa británico, que se la alquila a los Estados Unidos. Cuenta con 30 antenas, 12 de ellas con un diámetro superior a los 30 metros. Al menos una de las antenas grandes es una antena de recepción de comunicaciones militares (AN/FSC-78). Su cometido sería proporcionar transmisiones rápidas por radio e investigar las comunicaciones. Así mismo se habla de que, aparte de ser una estación terrestre para satélites espías, se encargaría también de la escucha de los satélites de comunicación rusos.

12. ***Bad Aibling*** (Alemania) 12°E, 47°N
Controlada por el NAVSECGRU, el INSCOM (66° IG, 718 IG) y varios grupos de la AIA (402° IG, 26° IOG). Consta de 14 antenas, todas menores de 18 metros. Los cometidos oficiales de esta estación son:
"Rapid Radio Relay and Secure Commo, Suport to DoD and Unified Commands, Medium and Longhand Commo HF& Satellite, Communication Physics Research, Test and Evaluate Commo Equipment".
Se encarga de los satélites SIGINT (espionaje electromagnético) y de las estaciones de escucha de los satélites de comunicación rusos. EL Departamento de Defensa de los Estados Unidos decidido cerrar esta estación el 30 de Septiembre del 2002 sin expresar motivo alguno.

13. ***Agios Nikolaos*** (Chipre) 32°E, 35°N
Consta de 14 antenas de tamaño desconocido. Controlada por Gran Bretaña en ella trabajan dos unidades: el "Signals Regiment Radio" y la "Signals

Unit" de la RAF. Es una estación muy próxima a Oriente Medio y es la única estación de esa zona de huellas de satélite.

14. ***Geraldton*** (Australia) 114°E, 28°S
Se encarga de ella el DSD (Servicio Secreto australiano) si bien los agentes británicos que se encontraban en Hong Kong hasta que esta ciudad pasó a formar parte de China ahora trabajarían en esta estación australiana. Cuenta con 4 antenas de 20 metros orientadas hacia el Océano Índico y el Pacífico Sur. Se ocuparía de la interceptación de satélites civiles.

15. ***Pipe Gap*** (Australia) 133°E, 23°S
Manejada por el DSD. Sin embargo la mitad de las 900 personas que trabajan allí son de la CIA y del NAVSECGRU. Posee 18 antenas satelitales de las cuales una es de 30 metros y otra de 20 metros. Es una estación para satélites SIGINT desde la cual se controlan varios satélites de espionaje cuyas señales se reciben y procesan. El tamaño de las antenas hace suponer que también se realizan interceptaciones de comunicaciones por satélite pues para los satélites SIGINT no es necesario el uso de grandes antenas.

16. ***Shoal Bay*** (Australia) 134°E, 13°S
Estación dependiente del Servicio de Inteligencia Australiano. Posee 10 antenas de tamaño no especificado aunque las más grandes podrían no sobrepasar los 8 metros de diámetro. Las antenas estarían orientadas hacia los satélites PALAPA indonesios. No está claro si forman parte o no de la red mundial de espionaje.

17. ***Guam*** (Pacífico Sur) 144°E, 13°S
Controlada por la 544° IG de la AIA y por la Marina de Estados Unidos. Alberga una estación naval de ordenadores y telecomunicaciones. Tiene 4 antenas, dos de ellas de unos 15 metros.

18. ***Waihopai*** (Nueva Zelanda) 173°E, 41°S
Estación controlada por el GCSB (General Communications Security Bureau de Nueva Zelanda). Consta de dos antenas, una de ellas de 18 metros

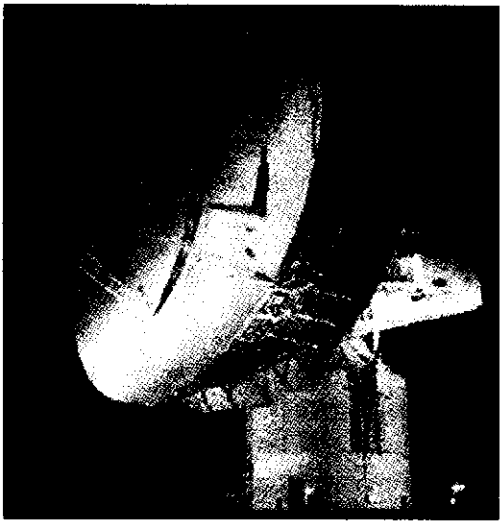
y sus funciones son la interceptación de comunicaciones por satélite y el procesado y descifrado de las transmisiones. Su pequeño tamaño y radio de acción (una pequeña parte del Pacífico) avala la hipótesis de una intercomunicación complementaria con la estación de Geraldton (Australia).

19. ***Hong Kong*** 22°N, 114°E
No se disponen de datos exactos referentes ni a su tamaño ni a su número de antenas. Sin embargo se sabe que posee varias antenas de gran diámetro. Tras la incorporación de Hong Kong por parte de China la estación fue suprimida. No se sabe cual de las estaciones cercanas ha asumido el papel que desempeñaba la estación de Hong Kong (Geraldton, Pipe Gap o Misawa). Todo hace parecer que las labores se repartieron entre varias estaciones.

20. ***Misawa*** (Japón) 141°E, 40°N
Controlada por Estados Unidos y Japón. Consta de 14 antenas, algunas de ellas de 20 metros. Es un centro de operaciones de criptología (Cryptology Operations Center) e intercepta las señales de los satélites rusos Molnyia y de otros satélites de comunicación también rusos.

Por qué se hace énfasis en el tamaño de las antenas. Porque las antenas de recepción terrestres tienen un tamaño comprendido entre 0,5 metros (como las parabólicas que se tienen en los tejados de algunas casas para la recepción de televisión digital). El sistema de recepción concentra la energía en el foco del espejo parabólico y dependiendo del tipo de emisión del satélite (la banda, la frecuencia, etc...) se necesitarán antenas parabólicas de mayor o menor tamaño. Cada sistema de satélites (dentro de lo posible, cada subsistema dentro de un sistema) consta de un tipo concreto de emisión y por lo tanto las antenas serán distintas, luego, cuando se pretende una obtención de información a través del filtrado realizado por un ordenador se usa una antena de tamaño máximo (20/30 metros). Las estaciones militares centrales suelen tener antenas de 18 metros, si bien se usan más pequeñas para facilitar la movilidad de las mismas permitiendo una movilidad táctica (estaciones móviles). Las estaciones que reciben

señales de satélites ***SIGINT*** (ondas electromagnéticas) y espías requieren antenas pequeñas, ya que las señales son de alta frecuencia y concentración. La presencia de 2 ó más antenas de 18 metros puede significar que allí se realizan escuchas de comunicaciones civiles.



GCHQ. «Shadow» esta estación ubicada en Gran Bretaña intercepta mensajes de Intelsat para UKUSA

Sin embargo algo que también permite intuir la actividad de una estación es la presencia o no de personal militar. De esta forma, si una estación con 2 ó más antenas de 18 metros alberga fuerzas armadas, alguna de las antenas podría dedicarse a comunicaciones militares. Un ciudadano normal nunca tendrá acceso a una estación de escucha, sea del tipo que sea. En las estaciones de escucha además siempre habrá presencia de personal militar.

De igual forma la disposición espacial y el tamaño y tipo de antenas puede mostrar el propósito de cada estación de escucha. De esta forma:

- Un conjunto de antenas verticales que forman un gran círculo se utiliza para averiguar la orientación de las señales de radio.
- Un conjunto circular de antenas romboidales tiene el mismo propósito.
- Las antenas direccionales o multidireccionales parecidas a las clásicas de televisión pero de tamaño gigantesco se usan para interceptar señales de radio no dirigidas.
- Las antenas parabólicas se utilizan exclusivamente para recibir señales.

La observación de una antena parabólica, fijándonos en su situación geográfica, su altitud y su orientación, podría desvelar la situación del satélite cuya señal se está recibiendo. Es por eso que estas antenas suelen mostrarse cubiertas por gigantescas esferas blancas, llamadas cúpulas. De esta forma, se ocultan la orientación e inclinación de la antena, y de paso se las protege de la intemperie.

LA POLÉMICA

El espionaje internacional practicado por la red Echelon no tiene límites. Todo el mundo está dentro de su campo de acción, todo el mundo está potencialmente destinado a ser espiado. Se da el caso curioso de que la legislación de Estados Unidos prohibe a la NSA (National Security Agency) el espionaje dentro de sus fronteras (que no en el resto del planeta), así que son los británicos los encargados de espiar a los Estados Unidos y luego se intercambian la información entre agencias. Sin embargo, a raíz de los atentados contra los Estados Unidos el 11 de septiembre del 2001 las leyes estadounidenses se están modificando para otorgar más poderes de espionaje interno a sus organismos de seguridad. Ejemplo de ello está el sistema ***CARNIVORE***, el cual lo dirige y supervisa el FBI. El objetivo del sistema es el de espiar la red de Internet entre otros servicios de telecomunicaciones local (Estados Unidos). Existe otro sistema de espionaje que se está gestando y cuyo principal artífice es el FBI en Europa, conocido con el nombre de ***ENFOPOL.***

La verdadera polémica nace cuando se acusa a los gobiernos implicados en el espionaje a través de Echelon de haberse extralimitado en sus acciones hacia el

espionaje industrial y político en beneficio de los gobiernos implicados en la red. Es curioso que con anterioridad ningún Gobierno recriminara la violación del derecho a la intimidad y privacidad del ciudadano común, lo cual se explica porque todos los gobiernos practican ese tipo de espionaje, además, no existe una legislación internacional que regule este tipo de acciones, a parte que no servirían de mucho cuando no existe ninguna igualdad y respeto a las leyes internacionales.

El ***Parlamento Europeo*** creó la Comisión Echelon a resultas de un libro publicado al respecto por el físico escocés Duncan Campbell (ver archivo anexo PDF en el cual Gerhard Schmid expone ante el parlamento Europeo su informe final sobre las funciones de la red Echelon en el viejo continente). El primer informe de esta comisión fue presentado en 1998 y en él se confirma la existencia de la red Echelon y su implicación en el espionaje a Gobiernos, organizaciones y empresas europeas. Es decir, que una tecnología con origen militar se está utilizando con fines económicos y de espionaje industrial para favorecer a empresas pertenecientes a países integrantes de la red en detrimento de empresas mayormente europeas y japonesas. Estas empresas no son cualquier empresa. Son empresas, principalmente norteamericanas, relacionadas directamente con la red Echelon y con el sistema defensivo y militar de los Estados Unidos, por ejemplo la firma aeronáutica McDonnell Douglas, o empresas punteras en campos tan críticos como telecomunicaciones, ingeniería genética o laboratorios de desarrollo de armas químicas y bacteriológicas. Esto se puede deber a que al gobierno de los EE.UU le interesa que esas empresas se mantengan fuertes, aunque la posibilidad más acertada sería que al estar esas empresas muy relacionadas con el Gobierno (por no decir que son una rama del mismo) sería ésta una forma más de controlar esos sectores tan importantes.

Se ha creado un gran revuelo e incluso Francia se plantea acusar formalmente a Gran Bretaña de traición a la Unión Europea, ya que sus acciones perjudican directa y conscientemente la economía de la Unión en beneficio de un enemigo comercial directo, como son los Estados Unidos. Se habla también de que Gran Bretaña podría estar violando la Convención de Derechos Humanos de la UE respecto a la privacidad. Gran Bretaña se defendió alegando que:

" sus leyes permiten espiar las comunicaciones para defender sus intereses económicos".

Estados Unidos, fiel a su tradición, negó todo conocimiento y Nueva Zelanda mostró su preocupación ante una más que posible investigación por parte de la Unión Europea de su base de escuchas en Waihopai, usada para el espionaje de la región del Pacífico, y aseguró que desde esas instalaciones no se realizan escuchas de «carácter comercial». Australia reconoció en 1999 la existencia de UKUSA y sus funciones, al igual que su pertenencia al mismo.

Actualmente se reconoce abiertamente la existencia de la red, si bien se niega que se utilice para realizar espionaje industrial y político, alegando que sus campos de acción son el terrorismo y las mafias del narcotráfico.

El espionaje industrial habría tenido su incursión con negativas consecuencias sobre varias corporaciones y empresas. Particulares franceses demandaron a los gobiernos de Gran Bretaña y Estados Unidos por robo de secretos industriales. Jueces y fiscales de Italia, Alemania y Dinamarca solicitan investigación pública sobre la red Echelon. Organizaciones norteamericanas como la Unión Americana de Libertades Civiles reclaman también una investigación.

A la Red Echelon se le atribuye, entre otras, acciones de carácter comercial y político como son:

- Interceptación y escucha de transmisiones de *Greenpeace* por parte de los Estados Unidos durante su campaña de protesta hacia las pruebas nucleares francesas en el Atolón de Mururoa en 1995. Este espionaje no fue conocido por sus socios más débiles, como Nueva Zelanda y Australia.
- Interceptación de llamadas telefónicas y posterior seguimiento a personajes como Lady Di, el Papa Juan Pablo II, Teresa de Calcuta, Amnistía Internacional y Greenpeace.
- Espionaje a dos ministros británicos por parte de Margaret Thatcher, siendo ella Primera Ministra del Reino Unido. Su objetivo era saber si estos dos

personajes eran espías, pues no estaban de acuerdo con ciertas formas de actuación de la dama de hierro.

- Espionaje del diario *Observer* (oposición) y a varios de sus periodistas y propietarios.
- La inteligencia militar francesa asegura que agentes secretos norteamericanos trabajan en la empresa ***Microsoft*** para instalar programas secretos en los productos e indicar a los que desarrollan programas para la misma empresa, qué agujeros de seguridad deben crear para que la NSA pueda entrar a través de ellos. Estos agujeros de seguridad se encuentran en productos como Windows e Internet Explorer. A cambio, recibiría apoyo financiero y se favorecería el monopolio del Microsoft en el mercado nacional e internacional, lo cual beneficia a ambas partes. Existe una llave conocida como ***NSAKEY***, que facilita una puerta trasera a la NSA para espiar y entrar a cualquier sistema operativo. Esta clave va abjunta al sistema Cripto API (Aplication programmer´s Interfase) de Windows, su función es validar el nombre de Microsoft y las firmas digitales de los nuevos programas que se quieren instalar en Crito API. La puerta trasera puede cargar programas en un PC sin autorización (Troyano) o Keyloggers Duros.
- Se asocia a la NSA la inclusión del denominado «cifrado fuerte» del Windows 2000 para fines tan desconocidos como preocupantes.
- Los sistemas de encriptación de mensajes de los productos Microsoft, Netscape y Lotus destinados al mercado europeo son distintos a los americanos y están predispuestos a ser decodificados por la NSA.
- La empresa informática Lotus reconoció que la NSA obliga a las empresas americanas a comunicarles una parte de la clave de codificación de los productos destinados al intercambio de mensajes que se exporten fuera de los Estados Unidos. En su caso, 24 de los 64 bits del código de desencriptación de los mensajes.
- La empresa suiza *Crypto AG*, expertos en programas, hardware y otros productos criptográficos (teléfonos móviles, por ejemplo) adjunta a los mensajes enviados a través de sus productos una clave de decodificación del password utilizado por el usuario que conocería la NSA. Se sabe que dicha empresa suiza y la NSA vienen manteniendo contactos y reuniones

desde hace unos 25 años. Los productos Crypto son utilizados por delegaciones oficiales de más de 130 países, tales como ejércitos, embajadas, ministerios, etc.

- Interceptación de comunicaciones entre Thomson-CSF y el Gobierno Brasileño en 1994 en la negociación de un contrato de 220.000 millones de pesetas para un sistema de supervisión por satélite de la selva amazónica permitió la concesión del proyecto a la empresa norteamericana Raytheon, vinculada a las tareas de mantenimiento de la red Echelon.
- Interceptación de faxes y llamadas telefónicas entre la empresa Airbus y el Gobierno de Arabia Saudí con detalles de las comisiones ofrecidas a los funcionarios, permitió a Estados Unidos presionar para que el contrato de un billón de pesetas fuera concedido a Boeing-McDonnell Douglas. 1995.
- Espionaje a la industria automovilista japonesa.
- Intercepción de la NSA de comunicaciones entre el Gobierno de Indonesia y representantes de la empresa japonesa NEC referentes a un contrato de 200 millones de dólares en equipamiento de telecomunicaciones. George Busch padre intervino personalmente y obligó a Indonesia a dividir el contrato entre NEC y la firma estadounidense AT&T (proveedora de equipamiento de telecomunicación a la NSA).
- Espionaje a las conversaciones entre países de Oriente Medio y representantes del consorcio europeo Panavia destinadas a la venta del cazabombardero Tornado a dichos países.

En Latinoamérica, aparte de Brasil, Argentina fue víctima de la red Echelon; existen serios rumores sobre intervenciones de comunicaciones, inclusive en su caída económica.

Un ingeniero de telecomunicaciones habría detectado que 21 líneas de teléfono del Ministerio de Economía de Argentina estaban siendo pinchadas desde el exterior, vía satélite. Se realizaron entonces revisiones de las líneas de teléfono del ministro y varios secretarios del ministerio. En estas revisiones se descubrió que todos los teléfonos pinchados lo estaban a través de un ordenador del mismo ministerio marca AST (empresa informática norteamericana que abastece

a la NSA de equipamiento). Investigando la computadora en cuestión se descubrió que tenía instalado un software denominado STG, el cual permite la intervención de líneas de fibra óptica, cable, teléfono, correo electrónico, fax y satélite.

El sistema basado en el software STG incluye un dispositivo de seguridad que es revisado y actualizado cada 24 horas por el mismísimo Departamento de Estado norteamericano y, para que el programa se mantenga activo, debe conectarse con el Pentágono diariamente. Este software sólo puede ser adquirido por organismos autorizados por el Departamento de Estado de los EE.UU. En Argentina, el único organismo autorizado es la SIDE (Secretaría de Inteligencia del Estado). Sin embargo, se comprobó que el pinchazo provenía del exterior de Argentina en una conexión vía satélite.

Dentro de la gravedad de esta red, el informe del Parlamento Europeo afirma que la red Echelon no es tan poderosa como se da a entender, al menos respecto a las comunicaciones a través de cable, si bien recomienda el cifrado y codificado de las comunicaciones vía Internet para mayor seguridad en la privacidad de individuos y empresas. Por otro lado, se aconseja de igual forma no utilizar programas de cifrado que hayan sido desarrollados ni en los Estados Unidos ni Gran Bretaña.

Así mismo, se consideran bastante seguras las comunicaciones realizadas a través de fibra óptica dentro de la Unión Europea, debido a la enorme dificultad que supone la interceptación de señales tan rápidas y de tan gran capacidad de datos, en otras palabras por su amplio ancho de banda.

Ahora cabe la pregunta. ***¿Por qué los gobiernos europeos no hacen algo contundente al respecto?.*** Bueno..., estos están igual o peor que la propia red Echelon, pues investigaciones realizadas por entidades europeas demostraron que, para citar un ejemplo los servicios secretos franceses consiguieron información privilegiada que permitió la concesión de un contrato a la firma aeronáutica gala Dassault. Todos los países poseen su sistema de espionaje, el cual

como es obvio no divulgan sus funciones específicas de trabajo, pero algo es seguro, sus usos no son solamente militar o en contra del delito, también se aplicará a la sociedad civil.

LUCHA CONTRA ECHELON

La lucha contra la red Echelon ha llegado también al ciudadano común, creándose un virus informático específico para esta red de espionaje llamado ***SEPRIN***. Se trata de un gusano que intentaría saturar los recursos de la misma. Aunque su efectividad aún no ha sido demostrada, pero existen otros sistemas informáticos como son los Spyhunter que anulan programas "troyanos" que merodean por la red atribuidos a Echelon.

Otros métodos planteados por Hacktivistas de la red de Internet es la de llamar la atención de la red Echelon, incluyendo nombres de personajes políticos de los estados unidos o países aliados, de directores de sus servicios de seguridad, de políticos extranjeros «enemigos», de terroristas, de equipos técnicos sofisticados, (informáticos de alto nivel), de productos altamente tóxicos, denominaciones de su armamento más moderno, lugares geográficos en donde existan conflictos, instalaciones militares o bases y similares.

La combinación de las palabras en un mismo texto, según un Hacktivista acentúa el efecto de rastreo de la red, por ello muchos manifestantes (Antiechelon), redactan documentos, en algunos casos incoherentes cuyo fin es involucrar la mayor cantidad de palabras clave (subversivas), para hacer "colapsar" el sistema haciendo perder horas máquina y horas hombre. Esta actividad se efectúa el día 21 de Octubre de cada año.

Cito un ejemplo extraído de Internet (La Casa de Jara) escrito por Jesús Parras:

Sr. PRESIDENTE de la Comunidad:
Le escribo para decirle que la BOMBA del agua se encuentra ATACADA por el óxido, por tanto sería conveniente CAMBIAR EL ESTADO de situación de la misma.
También quisiera informarle que la CASA BLANCA no está, sino -muy al contrario- la fachada presenta un ESTADO lamentable.
Además la puerta de entrada al garaje -(la que no se USA)- está rota y, para abrirla, es PRECISO DAR UN GOLPE DE MANO.
Convendría igualmente fumigar los DEPOSITOS puesto que según dice la vecina NORTEAMERICANA que vive en el 2º ha visto roedores que causan el TERROR entre la POBLACION infantil del vecindario.
Sería conveniente hablar con los padres del niño del 5º porque se pasa el día con la PISTOLA de agua, mojando a todos los vecinos.
Y, por si fuera poco, su hermano pequeño le CONTRA-ATACA con su MISSIL de plástico y su LASSER de goma espuma.
Aquello se convierte en un POLVORÍN juvenil y arrojan por las ventanas todos los juguetes BÉLICOS, tales como TANQUES, FUSILES, HELICOPTEROS, PORTAVIONES, SUBMARINOS, etc. etc. Y hasta alguna que otra BOMBA ATÓMICA.
Para terminar, recordarle que el domingo se casa la del 4º con su novio que es MILITAR, por si estima conveniente se decore la escalera.
Nota final: Le ruego haga copias de este escrito, («ECHELON» al correo) y lo haga seguir a todos, por si alguien nos vigila. Gracias.

¿HAY MÁS REDES PARECIDAS?

Como se enunció anteriormente existen redes de espionaje como el *Carnivore* y el *Enfopol*, avalados por estamentos gubernamentales de espionaje. Aunque en realidad existen desde tiempos ancestrales, lo que ha cambiado son los métodos y recursos de información y espionaje.

Según el informe Echelon de la Unión Europea, éstas son las modalidades de espionaje que practican los países de la Unión Europea y del consorcio UKUSA:

PAÍSES	Organización	Com. extranjeras (civiles, diplomáticas y militares)	Com. nacionales diplomáticas y militares	Com. nacionales civiles
Alemania	UE	SI	SI	SI
Austria	UE	SI	SI	NO
Bélgica	UE	SI	SI	NO
Dinamarca	UE	SI	SI	SI
España	UE	SI	SI	SI
Finlandia	UE	SI	SI	SI
Francia	UE	SI	SI	SI
Grecia	UE	SI	SI	NO
Holanda	UE	SI	SI	SI
Irlanda	UE	NO	NO	NO
Italia	UE	SI	SI	SI
Luxemburgo	UE	NO	NO	NO
Portugal	UE	SI	SI	NO
Suecia	UE	SI	SI	SI
Gran Bretaña	UE y UKUSA	SI	SI	SI
Australia	UKUSA	SI	SI	SI
Canadá	UKUSA	SI	SI	SI
Estados Unidos	UKUSA	SI	SI	SI
Nueva Zelanda	UKUSA	SI	SI	SI

La red ***ENFOPOL (Enforcement police- Policía de Refuerzo)***, fue creada para la interceptación de las telecomunicaciones en Europa, Estados Unidos, Australia y otros países. Enfopol nació en Bruselas en 1995, como una serie de requisitos técnicos para que las operadoras de telefonía adecuasen sus sistemas, ante eventuales demandas de «pinchazos» por parte de la policía.

Inicialmente Enfopol era llamado «*sistema EU-FBI*» y enlazaba «varias agencias de la ley como el Federal Bureau of Investigation (FBI), policía, aduanas, inmigración y seguridad interna». En 1998, oficiales de los ministerios de Interior europeos empezaron a discutir la ampliación de este sistema a Internet, telefonía móvil y fija (GSM) y nuevas formas de telecomunicación. Lo que implica según documentos desvelados, la garantía de un acceso fácil y «en tiempo real» a las comunicaciones, el tráfico -incluidos números marcados después de haberse cortado la llamada- y los datos -dirección IP, identificador de usuario, número de cuenta, contraseña, número PIN, dirección de correo, número de teléfono de quien llama, del que es llamado y de los que llaman al espiado, nombre completo y dirección, número de cuenta desde la que se paga el servicio - de los usuarios de servicios móviles terrestres, Internet (correo electrónico, Web, FTP, IRC, etc.), servicios de larga distancia e internacional, de datos, correo de voz, al igual que incluye el intercambio de resultados de análisis de ADN. Todo, montado por los propios operadores de redes y proveedores de servicio, quienes deben aportar la interfase de interceptación.

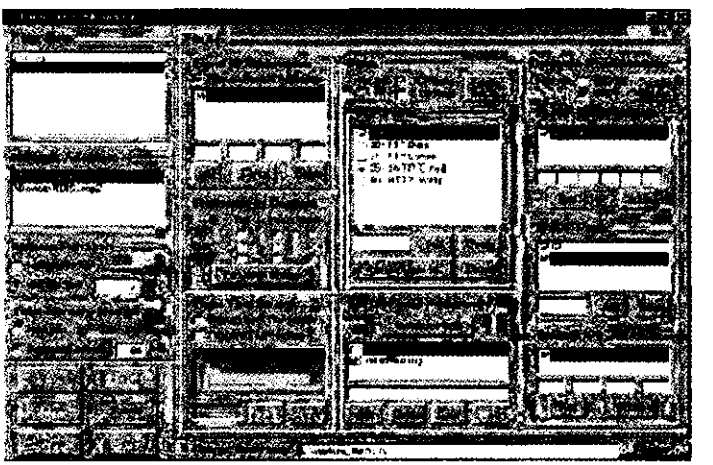
Un informe de la «*An Appraisal of Technologies of Political Control*» de la oficina Scientific and Technologies Options Assessment (STOA), presentado en el año de 1998 al Parlamento Europeo, bajo los nombres ***Enfopol, Echelon o Wassenaar*** se esconden «reuniones de las fuerzas operativas de un nuevo estado global de inteligencia militar» y policial. Desde este punto de vista, lo que se está tejiendo es el control, sin fronteras de estados o criptológicas, del primer mundo telecomunicado, con Estados Unidos al frente y Australia y Europa secundándolos.

Se atribuye también redes parecidas a países como Francia (conocida como ***Frenchelon***) y Rusia (que se llamaría ***Sorm***), debido a sus situaciones geográficas y al control y capacidad de actuación que poseen sobre sus «antiguas colonias». Suiza tiene su propia red, llamada ***Satos 3***.

Sin ser un sistema de redes, también es famosa la herramienta ***CARNIVORE***, sucesora del sistema *Omnivore*, desarrollada por el FBI y cuya finalidad es la de espiar la información que circula por Internet: desde páginas visitadas

hasta correos electrónicos, pasando por archivos transferidos, también incluye sistemas de fax y comunicaciones móviles y fijas.

El FBI viene instalando las ***"cajas negras"*** del sistema Carnivore en las computadoras de los proveedores de servicio de Internet (ISP), que proveen la conexión a la red de Internet para compañías de Internet como AOL y MCS, además de universidades, corporaciones y dependencias públicas.



La figura presenta de una ventana para configuración del Carnivore, donde se analiza la fuente del código o información y el destinatario entre otros.

El FBI asegura que Carnivore está diseñado para proteger a las personas inocentes y su privacidad, de forma que tan sólo recoge aquella información que es considerada peligrosa y que atenta contra las leyes. Hasta el momento, según fuentes del FBI, el sistema Carnivore ha sito utilizado en casos criminales, y en casos de seguridad nacional relacionados con espionaje o terrorismo.

Carnivore ha sido diseñado por el FBI como una solución completa similar a una caja negra tipo «Plug & Play». Además del software, el FBI incluye el hardware compuesto por un PC ensamblado en una caja modelo «rack» para

que pueda incorporarse de forma fácil en las redes de los ISP, como si de un concentrador o un router más se tratara, sin necesidad de contar con dispositivos externos como un ratón o teclado.

En el apartado técnico, el sistema está formado por un programa que actúa como «sniffer», diseñado por el gobierno aprovechando el software comercial. La función de un «sniffer» consiste en escuchar el tráfico que circula por una red capturando todos los paquetes de datos que viajan por ella. Este tipo de herramientas las utilizan los administradores para llevar a cabo análisis y diagnósticos del tráfico de las redes y por supuesto para el espionaje.

En lo que respecta al uso que se le ha dado de momento a Carnivore, su principal atención se centra en monitorizar los mensajes de correo electrónico en busca de información considerada de alto riesgo por el FBI. Aunque técnicamente puede llegar a controlar todo el tráfico que circula por cualquiera de los protocolos utilizados en Internet, hasta el momento tan sólo se ha ampliado su capacidad a la interceptación de sesiones FTP.

Otra característica que diferencia al sistema Carnivore de otros «sniffers» similares es que se configura para espiar el correo de entrada y de salida de usuarios sospechosos, teniendo en cuenta los campos «to» y «from» de la cabecera de los mensajes, ignorando el contenido de los mensajes del resto de usuarios. Este método es más selectivo que el utilizado por los «sniffers» con propósitos similares que realizaban búsquedas de términos considerados sensibles, como por ejemplo «terrorismo» o «droga», en el cuerpo de todos los mensajes a los que tenía acceso, por lo que el tráfico capturado era mucho mayor y en muchas ocasiones daba lugar a equívocos (versión similar a Echelon).

Algunas entidades civiles han solicitado que se haga público el código fuente de Carnivore, para someterlo a un estudio, de tal manera que pueda verificarse su transparencia con respecto a la privacidad de los usuarios. El FBI se ha negado a esta petición argumentando que la publicación del código fuente permitiría a los criminales estudiarlo para crear sistemas de comunicación que no puedan ser capturados.

Otra herramienta supuestamente utilizada por el FBI sería el troyano **NetBus**, uno de los más poderosos de hoy en día. Los enlaces de Seguridad no han podido confirmar la veracidad de esta afirmación.

Recientemente la **CIA** se ha hecho con otra herramienta de similares características a la red Echelon, si bien en vez de utilizar palabras clave, se vale de conceptos. No se descarta que este software sea aplicado también para su uso en la red Echelon, sobre todo si se tiene en cuenta que la empresa desarrolladora del mismo se encuentra en Mountain View (California, EE.UU.), sede de uno de los nodos de la red Echelon, lo cual hace sospechar la independencia de dicha firma informática respecto del Gobierno de los Estados Unidos.

Hace poco se ha sabido que el FBI está desarrollando un nuevo troyano, llamado Magic Lintern (**Linterna Mágica**). Donde el FBI está presionando a las empresas que desarrollan software antivirus y antitroyanos para obligarlas a que sus respectivos productos no detecten dicho troyano. En teoría hasta ahora ninguna de estas empresas ha dado el visto bueno, aunque hay rumores que Symantec (productos Norton) como Network Associates (productos McAfee) han claudicado a las presiones el Gobierno Estadounidense. Sin embargo, su postura oficial es que sus productos no van a permitir el paso del troyano. Básicamente circulan esos rumores porque son empresas estadounidenses y porque son punteras mundialmente. Además de ellos, se sabe que los que desarrollan los sistemas de protección viral informático contra Echelon como AVP y Sophos entre otras, se han negado a la propuesta del FBI, al igual que la nipona Micro Trend (PC-Cillin). Pero queda el beneficio de la duda, que tan cierto puede ser esto, a sabiendas que las empresas son norteamericanas. En su mayoría.

Ahora bien no se comprende por qué hay que dejar que el FBI introduzca un troyano en los PC de los usuarios de Internet, cuando a un hacker no se le permite y castiga con prisión.

Es cuestión de tiempo que un hacker o cracker deduzca el código del troyano y lo difunda por la red, todas las computadoras estarán específicamente desprotegidas ante ellos. O se puede crear un troyano que se haga pasar por el Linterna

Mágica y se estaría en las mismas. Ya se sabe que en estos temas, la imaginación es la mejor arma. Es más, ya han surgido troyanos que se hacen pasar por la Linterna Mágica, como el Magic Latern, aunque éste tan solo le «copia» el nombre.

REFLEXIÓN

En estados unidos una mayoría de la sociedad civil no está de acuerdo con las acciones de Echelon y Carnivore, de ahí que varias entidades pro derechos humanos como la unión Americana de Libertades Civiles ACLU, promueve marchas proechelon, esta información se puede ubicar en un página de internet (**ECHELONwatch**), donde se explica con precisión la historia del sistema, su funcionamiento, la legislación sobre la materia e informes varios muy completos. Además desde el sitio se puede completar un formulario para reclamar a las autoridades norteamericanas el "blanqueo" y eliminación del sistema.

La premisa de la ACLU se sintetiza en el siguiente recuadro.

> We at EchelonWatch are deeply saddened by the terrible events of September 11. We extend our deepest sympathies to the victims and their families.
> We support vigorous and appropriate actions by intelligence and law enforcement agencies to prevent more attacks from taking place. The goal of EchelonWatch is not to disband legitimate intelligence operations but to insist that they be subject to proper oversight.
> It is now more important than ever to subject powerful surveillance systems to the proper oversight and control by the institutions of democratic government. Effective operation against terrorists and strong oversight are not at all incompatible. We expect that in the coming months, the redoubled effort to prevent terrorism will lead to an expansion of Echelon and the related communications surveillance systems. Unfortunately, history shows that times of national crisis are often accompanied by enormous pressure to expand surveillance in ways that threaten privacy and civil liberties without enhancing security, such as spying on lawful political activities.
> That is why Congress and the democratic institutions of other nations must take their oversight responsibilities more seriously - making sure not just that the system is effective, but also that its capabilities are well understood, and that it isn't used to violate our privacy and civil liberties.

Los problemas Bioéticos de la Red Echelon y en general de todos los sistemas de espionaje mundiales atentan contra la dignidad humana y contra la intimidad, en lo concerniente a los principios de la bioética como son la ***no maleficencia*** (No hacerle daño o mal al otro. Echelon atenta contra toda la humanidad, lastimando su dignidad e intimidad humana), ***beneficencia*** (Acción buena - donde es más valiosa para el que la recibe que para el que la da. En el caso que nos ocupa no hay tal), ***justicia*** (Se considera como equidad con relación a los grupos sociales, en donde recursos y bienes comunes se distribuyen de manera equitativa y participativa por parte de cada individuo. Cuando se adecua a la ley a un principio general, norma o criterio. Para Echelon es imposible, pues aun con sus propios socios retiene información que nunca compartirá, usándola para beneficio propio) y ***autonomía*** (es sinónimo de independencia, originalidad y capacidad de cada persona en poder decidir en las cosas que le son propias de acuerdo a sus intereses, responsable de sus propios actos, distinguiendo lo bueno de o malo. Es la expresión del sentido de dignidad humana. Si se tiene en cuenta cada palabra escrita del significado de autonomía, es evidente que los servios de espionaje, en particular la red Echelon pisotea la autonomía del ser, coaccionando la libertad de expresión de manera directa o indirecta sin que la persona se percate de ello, hasta que es demasiado tarde).

Los gobiernos se escudan en que estos sistemas defienden sus países contra agresiones externas, pero no justifican por que rastrean clandestinamente los servicios de telecomunicaciones que usan sus compatriotas sin que ellos se percaten. Además no existe una legislación mundial al respecto, haciendo que las personas fuera de estos países se hallan indefensas. Es claro que este hecho es injustificable, más aún es no saber, cuantas personas han sido privadas de su libertad por ser sospechosos de agredir a cualquier potencia en forma verbal o escrita. Ningún ciudadano en el mundo puede estar a salvo de esta telaraña invisible que posee ojos en tierra, mar, aire y espacio.

Para finalizar este trabajo dejo una frase como reflexión, dirigida a las grandes organizaciones de espionaje mundiales y a las personas del común que no tienen idea que son monitoreadas constantemente a través de la red de Internet o cualquier servicio de telecomunicación mundial.

"Amonestar a un hombre obstinado en el mal (Echelon), es lo mismo que poner un espejo delante de un ciego". Proverbios.

¿Qué acciones debemos seguir?. La respuesta está en como interpretemos esta frase.

BIBLIOGRAFÍA

- http://www.seprin.com/echelon.htm
- http://altavoz.nodo50.org
- http://www.arnal.es/free
- http://www.telepolis.de
- http://www.ecn.org/lists/cyber-rights/
- http://www.seprin.com/virus_logico.htm_
- http://www.clarin.com/diario/echelon/
- http://www.clarin.com/diario/2000-02-28/i-02401d.htm
- http://www.lahaine.f2s.com/Internacional/red_imperialistas.htm
- http://es.gsmbox.com/news/mobile_news/all/59510.gsmbox
- http://www.rebelion.org/cultura/red_echelon180401.htm
- http://ar.clarin.com/diario/2001-05-20/s-05702.htm
- http://www.lanacion.com.ar/01/05/30/dx_308783.asp
- http://www.idg.net/english/crd_parlamento_693606.html
- http://www.argo.es/~jcea/artic/hispasec47.htm
- http://www.argo.es/~jcea/artic/hispasec48.htm
- http://www.rnw.nl/informarn/html/act010605_echelon.html
- http://www.antorcha.org/hemer/echelon.htm
- http://www.izquierda-unida.es/InformacionComunicacion/AgenciasPrensa/

- http://www.arrakis.es/~1alex/echelon.htm
- http://www.ccoo.upv.es/Personales/Echelon/echelon2000.htm
- http://altavoz.nodo50.org/mas_echelon.htm
- http://commons.somewhere.com/rre/1999/RRE.Echelon.html
- http://www.lainsignia.org/2001/mayo/cyt_009.htm
- http://www.terra.es/internet/articulo/html/int2164.htm
- http://www.el-mundo.es/2000/02/25/sociedad/25N0083.html
- http://www.cnn.com/2001/TECH/internet/07/30/echelon.protest/index.html
- http://www.el-mundo.es/navegante/2001/03/08/seguridad/984041457.html
- http://www.lugcos.org.ar/juanjo/echelon.htm
- http://www.aclu.org/echelonwatch/
- http://www.monde-diplomatique.fr/dossiers/echelon/
- http://www.europarl.eu.int/tempcom/echelon/rrechelon_en.htm
- http://www.intelsat.com
- http://www.intersputnik
- http://www.inmarsat.com
- http://www.panamsat.com
- http://ww.eutelsat.com
- http://www.arabsat.com
- http://www.aclu.org/
- http://www.epic.org/
- http://es.gsmbox.com/news/mobile_news/all/58158.gsmbox
- http://www.clarin.com.ar/diario/2000-02-27/i-03602d.htm
- http://www.gwu.edu/~nsarchiv/
- http://www.theage.com.au/daily/990523/news/news3.html
- http://sunday.ninemsn.com.au/sun_cover2.asp?id=818

- http://www.freecongress.org/ctp/echelon.html
- http://www.hispasec.com/unaaldia.asp?id=171
- http://www.europarl.eu.int/dg4/stoa/en/publi/publi.htm
- http://www.jya.com/echelon.htm
- http://www.heise.de/tp/deutsch/special/enfo/11818/1.html
- http://www.fipr.org/polarch/enfopol19.html
- http://www.fas.org/irp/eprint/sp/sp_lc2.htm
- http://www.ugr.es/~aquiran/cripto/enfopol.htm
- http://www.iptvreports.mcmail.com/stoa_cover.htm
- http://fire.net.nz/echelon.htm
- http://www.inforvip.es/jara/index.html
- www.inforvip.es/jara/masheespi.html
- http://www.derechos.org/nizkor/colombia/libros/redes/index.html
- http://www.derechos.org/nizkor/colombia/libros/redes/4.html
- http://www.kriptopolis.com/
- *www.sophos.com/virusinfo/articles/echelon.html*
- http://www.sophos.com
- http://www.rwur.org
- http://www.sophos.fr
- http://www.sophos.de
- http://www.esp.sophos.com
- http://www.gcsb.gov.nz
- http://www.dsd.gov.au
- http://www.NSA.org
- http://www.cse.dnd.ca
- http://www.gchq.org.AK

- http://www.echelonwatch.org/
- Privacidad según el Equipo Nizkor http://www.derechos.org/nizkor/espana
- Global Internet Liberty Campaign - GILC (Main issues: free speech, privacy, cryptography, access) http://www.gilc.org/
- Global Internet Liberty Campaign Member Statement on «Human Rights and the Internet» (Prepared for a one day briefing session for Members of the European Parliament, 27th January 1998, in Brussels) http://www.ozemail.com.au/~mbaker/europ-hr.html
- Echelon Watch http://www.aclu.org/echelonwatch/index.html
- «85 recommandations pour un Internet démocratique en l'an 2000» Contribution d'IRIS à la consultation gouvernementale «Cadre législatif de la société de l'information» Rapport IRIS - Novembre 1999 http://www.iris.sgdg.org/documents/rapport-lsi/
- Report on International Status of Privacy: «Privacy and Human Rights 1999». Electronic Privacy Information Center Washington, DC, USA. Privacy International London, UK http://www.privacyinternational.org/survey/
- «Cryptography and Liberty 1999: An international Survey of Encryption Policy». Electronic Privacy Information Center Washington, DC http://www2.epic.org/reports/crypto1999.html#_Toc450793110
- «An Appraisal of Technologies of Political Control». Scientific and Technological Options Assessment - STOA. 06jan98. http://cryptome.org/stoa-atpc.htm