LA RED Echelon: PRIVACIDAD, LIBERTAD Y CRIPTOGRAFIA

Germán Pachón Ovalle
Programa de Doctorado en SIC
Universitat Oberta de Catalunya
Barcelona
01/06/04

Introducción

El trabajo se propone revisar el desarrollo del proyecto Echelon, los efectos que genera su aplicación y la reacción de países, comunidades y personas frente al problema de la privacidad y la libertad en las comunicaciones electrónicas, particularmente por la Red INTERNET.

Aunque fue producto de la guerra fría –y ella supuestamente ya concluyó- , el proyecto Echelon ha ido convirtiéndose en una acción político-militar de gran envergadura, dictada por USA, sobre los sistemas de comunicación electrónica en el planeta, inicialmente justificada con el argumento de la seguridad nacional y desde el 11/9 como esencia de la lucha contra el terrorismo.

Los nuevos desarrollos de la red Echelon, sus efectos previsibles en los individuos, las comunidades, las empresas y los países, ha generado una reacción importante que se expresa por ejemplo en América con las acciones de la ACLU (American Civil Liberties Union) y la advertencia del surgimiento de la "American Surveillance Society", y en Europa con las acciones de Gobiernos y comunidades por el espionaje político, doméstico, industrial y comercial en que ha derivado presumiblemente su acción.

Si bien Echelon no es el único sistema de espionaje existente, si constituye el proyecto que ha efectuado mayor número de acciones no legales, evidentes, sobre países y empresas, y tal vez personas, en el transcurso de los últimos años. Todo indica que Echelon es un proyecto esencial en la construcción de una nueva forma de imperio universal basada en el manejo de la información.

El trabajo aborda finalmente la utilización de tecnología contra los propios desarrollos tecnológicos que contiene el proyecto Echelon. En tal sentido, se revisan las propuestas en criptografía, particularmente con el PGP, como formas de evadir o contrarrestar el efecto del espionaje en las comunicaciones sobre las libertades personales y sociales.

1. ¿Qué es el proyecto Echelon? Evidencias de su existencia

La red ultrasecreta Echelon se creó a principios de los años 70 y fue ampliada y fortalecida entre los años 1975 y 1995. Está dirigida por la NSA (National Security Agency) norteamericana y la Agencia Británica de Comunicaciones Gubernamentales (GCHQ).

Oliveras et al. [1]dicen que "*echelon es un sistema tan real como poderoso, y tan eficaz como desconocido… es un sistema de interceptación, clasificación y evaluación de las telecomunicaciones. Si fuese solamente eso, no se diferenciaría de otros esquemas similares puestos en marcha por los sistemas de espionaje de todo el mundo. Pero tiene algunas características que lo hacen único:*

En primer lugar, es internacional tanto en ámbito como en composición. Echelon está formado por un "consorcio" de diversas naciones: EEUU, Reino Unido, Canadá, Australia y Nueva Zelandia. Cada uno de estos países tiene un campo de actuación y comparte con los otros miembros del club sus descubrimientos. Este proceder, además de asegurar una mayor cobertura, permite evadir espinosos problemas legales: puesto que la NSA norteamericana tiene prohibido por ley espiar dentro de los Estados Unidos, le basta con pedir la información a sus colegas del Reino Unido o de Canadá para obtenerla. No suelen darse muchos casos de Espías S.A. pero parece que este funciona, y además da buenos dividendos a sus accionistas.

En segundo lugar, Echelon fue diseñado para que se comporte como una entidad inteligente. No se limita a interceptar mensajes y re-transmitirlos, ya que el enorme volumen de comunicaciones existente lo haría inviable. Por ello, se ha apelado a procedimientos informatizados de reconocimiento de voz y de contexto, y de búsqueda de palabras. Los mensajes intervenidos son cotejados en un "diccionario" en busca de concordancias. Si se halla alguna (digamos si un mensaje incluye las palabras Clinton y Asesinato), el mensaje es enviado a donde corresponda. Es como una red de deriva inteligente, que solamente captura los peces que le interesa. Claro que los peces, ignorantes de la existencia de la red, siguen su camino creyéndose a salvo.

En tercer lugar, y a diferencia de otros muchos sistemas, Echelon fue diseñado específicamente para captar y procesar grandes cantidades de información en redes de transmisión CIVILES. Es decir, si Echelon está espiando comunicaciones comerciales y particulares no es porque se haya reconvertido tras el final de la guerra fría; simplemente, sigue haciendo el trabajo para el que ha sido diseñado. Las redes de telecomunicaciones militares ya tienen sus espías electrónicos. Echelon se ocupa del filón de las comunicaciones civiles: telefonía fija, móvil, fax, Internet... Como dicen los americanos "usted lo nombra, yo lo tengo".

Estas tres características lo hacen un sistema eficiente que puede definirse como un "conglomerado político-económico al servicio de determinado trust"[2], o imperio, pues proporciona la información suficiente y necesaria para que las compañías norteamericanas tengan un control absoluto de los negocios del mundo y la información política para que USA tome las medidas que considere necesarias para mantener su dominación mundial.

Echelon es la palabra clave para designar un sistema automatizado de interceptación global y de comunicación, operado por los servicios de inteligencia y espionaje de los países que lo constituyeron inicialmente. Tiene su origen en el acuerdo semi-secreto UK-USA (Gran Bretaña-Estados Unidos) firmado inicialmente en 1947, teniendo como principal cliente la CIA, pero con el fin de la guerra fría se convirtió en una red para usos civiles y económicos. El Echelon original data de 1971 y su nombre fue establecido por la NSA. Para la Lockheed Martin el código alfanumérico de la red era p415.

USA, Reino Unido, Canadá, Australia y Nueva Zelandia parecen tener un nombre clave diferente para el mismo proyecto[3]. Mientras en USA es la NSA (Nacional Security Agency) es quien lidera la red, en Australia

---

[1] OLIVERAS, Eliseo y Antonio Fernández. (2001). *La traición de Londres: nuestros socios y aliados nos espían.* En http://www.tiempodehoy.com

[2] op. Cit.

[3] BLADET, Ekstra. (1999). *Echelon.* Entrevistas con Margareth Newsham ex-agente de la NSA en Echelon.

es la DSD (Defence Signals Directorate), en el Reino Unido el GCHQ (Government Communications Headquarters), en Canadá el CSE (Communications Security stablishment), la GCSB (General Communications Security Bureau) de Nueva Zelanda y las agencias de inteligencia y espionaje de los aliados de Estados Unidos, según el contenido de varios tratados[4].

Echelon es un término inglés que significa "escalón", aunque esta red también es conocida como "la gran oreja".[5] Como tal es un programa informático, pero como red es un entramado de antenas, estaciones de escucha, radares, satélites, submarinos y aviones espía, unidos todos estos elementos a través de bases terrestres, cuyo objetivo es espiar las comunicaciones mundiales, teóricamente para la lucha contra el terrorismo internacional y el tráfico de drogas.

El campo de acción de la red es el mundo y el espionaje practicado por ella parece no tener límites. Aunque los gobiernos de los cinco países mencionados no confirman su existencia, a partir de 1988 cuando la Unión Europea creó la Comisión Echelon como respuesta al libro publicado por el Físico escocés Duncan Campbell[6] sobre este tema, se acepta su existencia y se genera una gran polémica sobre los excesos de quienes operan la red, al haber avanzado hacia el espionaje industrial y político, en beneficio de los gobiernos de estos cinco países o de sus compañías relacionadas con el proyecto.

Los dos informes de la Comisión Europea sacaron a la luz pública una cantidad preocupante de pruebas que sugieren que el poder de Echelon puede haber sido sub-estimado. El primer informe titulado "Una evaluación de las tecnologías del control político" (An appraisal of technologies of political control)[7], sugería que Echelon tuvo a civiles como su principal objetivo.

El informe reveló que**:**

"El sistema ECHELON forma parte del sistema UKUSA, pero al contrario que muchos de los sistemas de espionaje electrónico desarrollados durante la guerra fría, ECHELON está diseñado principalmente para objetivos civiles: gobiernos, organizaciones y negocios en virtualmente cualquier país. El sistema ECHELON funciona mediante la intercepción indiscriminada de enormes cantidades de comunicaciones, de las que se desvían aquellas valiosas con la ayuda de programas de inteligencia artificial como MEMEX - destinados a encontrar palabras clave. Cinco naciones comparten los resultados con los Estados Unidos como país líder bajo el pacto UKUSA de 1948. Gran Bretaña, Canadá, Nueva Zelanda y Australia actúan como servicios de información subordinados.

"Cada uno de los cinco centros proveen a los otros cuatro "diccionarios" de palabras, frases, gente y lugares para "etiquetar", y así la intercepción de lo etiquetado se dirige directamente al país que lo pidió. Mientras que hay mucha información obtenida de terroristas potenciales, hay también mucho espionaje económico, y una intensiva monitorización de todos los países participantes en las negociaciones del GATT. Pero Hager encontró que la principal de las prioridades de este sistema continuó siendo respecto a objetivos militares y políticos aplicables a sus amplios intereses. Hager cita a un "alto operario de Inteligencia" que habló en el Observer en Londres. "Sentimos que no podemos seguir más tiempo callados respecto a lo que consideramos

---

Traducido por Wintermute.

[4] CAMPBELL, Duncan. (1999). *Interception capabilities 2000.* En: http://www.iptvreports.mcmail.com/stoa_cover.html

[5] VARIOS AUTORES. (2002). *La gran oreja: red de satélites espía de la US National Security Agency (NSA). Países anglosajones espían Europa.* En http://www.enlaces

[6] CAMPBELL, Duncan. (1988). *Alguien está escuchando.* New Statesman, 12 de agosto. En: http://jya.com/echelon-dchtm

[7] ver WRIGHT, Steve. (1988). *An appraisal of technologies for political control.* En: http://cryptome.org/stoa-atpc.htm

un procedimiento flagrantemente ilegal y negligente respecto al sistema político en que operamos.". Dieron como ejemplos la intercepción por parte del GCHQ de tres ONGs, incluyendo Amnistía Internacional y Christian Aid. "En cualquier momento GCHQ es capaz de entrar en sus comunicaciones para la obtener de modo rutinario un objetivo," dijo la fuente del GCHQ. En el caso de los pinchazos telefónicos el proceso es conocido como Mantis. Con telex se denominan Mayfly. Mediante el tecleo de palabras clave relativas a la ayuda al tercer mundo, la fuente fue capaz de demostrar "arreglos" en el télex en las tres organizaciones. Sin nadie a quien pedir responsabilidades, es difícil descubrir que criterio determina quién no es un objetivo." El informe más reciente, conocido como "Capacidades de Intercepción 2000", describe la capacidad de ECHELON en un detalle incluso más elaborado que antes.

Además, un funcionario oficial del gobierno italiano ha comenzado a investigar los esfuerzos de búsqueda de información de ECHELON, basándose en la creencia de que la organización puede estar espiando a los ciudadanos europeos violando las leyes italianas e internacionales

El parlamento Danés también ha iniciado una investigación.

Los acontecimientos en Estados Unidos indican que el "muro de silencio" no durará mucho más. Ejerciendo su descuidada autoridad constitucionalmente creada, miembros del "House Select Committee on Intelligence" comenzaron a hacer preguntas recientemente sobre la base legal de las actividades de ECHELON por parte de NSA. En particular, el Comité quería saber si las comunicaciones de ciudadanos americanos estaban siendo interceptadas y bajo qué autoridad, ya que la ley de este país limita la capacidad de sus agencias de inteligencia respecto a su propio país. Cuando fue preguntada sobre su autoridad legal, la NSA invocó el privilegio abogado-cliente y rechazó revelar los standards legales en los que ECHELON debe haber conducido sus actividades.

El Presidente Clinton ha firmado una ley de fondos que debería, como mínimo, obligar a la NSA a dar cuentas de la base legal para ECHELON y actividades similares.

Además, el republicano Bob Barr (R-GA), quien ha tomado el liderazgo en los esfuerzos del Congreso para obtener la verdad acerca de ECHELON, ha mostrado su conformidad con la "House Government Reform" y el "Oversight Committee" para controlar las escuchas "por descuido".

Finalmente, el EPIC (Electronic Privacy Information) ha presentado una demanda contra el Gobierno de EEUU, esperando obtener documentos que describan los standards legales bajo los cuales opera ECHELON."

El informe más reciente, el segundo, describe al detalle las capacidades de la red Echelon.

Abierta la polémica, la comunidad se centró en los temas de:

- Las firmas norteamericanas relacionadas con el sistema de defensa y militar, como por ejemplo la McDonnel-Douglas y empresas punteras en campos como las telecomunicaciones, ingeniería genética o laboratorios de desarrollo de armas químicas o bacteriológicas.
- Francia se plantea acusar formalmente al Reino Unido de traición a la Unión Europea, ya que sus acciones en este campo privilegian a un enemigo comercial de la Unión como es USA, en detrimento de la economía europea.
- Gran Bretaña podría estar violando la convención de Derechos Humanos de la UE respecto a la privacidad.
- El espionaje industrial parece haber tenido consecuencias negativas sobre varias corporaciones y empresas no relacionadas con la red.
- Jueces y fiscales de Italia, Alemania y Dinamarca solicitan una investigación pública sobre la Red Echelon.
- La ACLU americana reclama también investigaciones al respecto.
- Otras entidades como Greenpeace, diarios como The Observer y personajes mundiales parecen haber sido objeto de interceptación de sus comunicaciones.

En documentos como *La Gran Oreja* [8] se le atribuyen a la Red Echelon una serie de acciones de espionaje comercial y político como:

- **"***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 Muroroa en 1995. Este espionaje no fue conocido por sus socios más débiles, como Nueva Zelanda y Australia.*
- *Interceptación de llamadas telefónicas y seguimientos a 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.*
- *Espionaje del diario Observer y a varios de sus periodistas y propietarios.*
- *La inteligencia militar francesa asegura que agentes secretos norteamericanos trabajan en la empresa Microsoft (el que faltaba) para instalar programas secretos en los productos e indicar a los desarrolladores de programas de Microsoft 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.*
- *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 los la NSA.*
- *La empresa informática Lotus reconoce 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 des-encriptación 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, ... Parece ser que aún seguimos sin poder fiarnos de los suizos... que se lo pregunten a los judíos.*
- *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 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 Bush 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).*

[8] Op. Cit.

- *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 Argentina también hay serios rumores sobre intervenciones de comunicaciones.

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."

Estas acciones denunciadas por los propios afectados son evidencias de la labor de espionaje y la intromisión en las comunicaciones privadas, pero la entrevista que realizara la periodista Ekstra Bladet [9] a la exagente de la NSA en Echelon Margareth Newsham, revela datos irrefutables sobre su existencia y sus actividades. Su actividad profesional por 10 años estuvo dedicada a empresas como Signal Science, Ford Aeroespacial y Lockheed Martin; desarrolló y actualizó satélites para Echelon y ordenadores que las compañías diseñaron para la NSA.

2. Estructura y Componentes de la red Echelon

La red es un complejo de dispositivos satelitales, computadores, software especializado, antenas de escucha, estaciones facilitadoras y procesadoras, aviones, barcos, submarinos y personal entrenado, que cubre todo el planeta.

Para el 2003 el presupuesto asignado para la NSA es de 3.600 millones de euros y mantiene bajo su control 120 satélites militares.

Un detalle de sus componentes es el siguiente:

Satélites Militares

- MILSTAR. (USA). Gestiona 6 satélites geoestacionarios para comunicación militar a nivel mundial con navíos, bases terrestres, aviones, barcos y submarinos.
- DSCS. (USA). Compuesto por 5 satélites para comunicación global
- SKUNET. (UK). Sistema de cobertura mundial.
- SYRACUSE. Francés de alcance regional
- SICRAL. Italiano de alcance regional
- SISTEMA ESPAÑOL (¡?). De alcance regional que utiliza la banda X de los satélites civiles como es el caso del francés y del italiano.
- MOLNYIA. Ruso que utiliza también la banda X
- OTAN. Las series de satélites NATO IIID, NATO IVA y NATO IVB

Satélites espías

Según MSNBC y NBC News[10], la red Echelon tiene un sistema especial adicional de satélites espías de uso permanente. Ellos se indican en la tabla 1.

[9] BLADET, Ekstra. (1999). *Echelon.* Entrevistas con Margareth Newsham ex-agente de la NSA en Echelon. Traducido por Wintermute.

[10] VINDREM, Robert. (1998). *Spy satellites enter new dimension.* MSNBC y NBC News, August 8.

Tabla 1. Satélites espías permanentes de USA

SATELITE	No.	ORBITA	CONSTRUCTOR	PROPOSITO
Advanced KH-11	3	200 miles	Lockheed Martin	5¨resolution photo
LaCrosse Radar Imaging	2	200-400 m	Lockheed Martin	3-10 feet R.Ph.
Orion/Vortex	3	22.300 m	TRW	Telecom Surv.
Trumpet	2	200-22.300m	Boeing	Surv. Cel. Phones
Parsae	3	600 m	TRW	Ocean Surv.
Satellite Data Systems	2	200-22.300m	Hughes	Data Relay
Defense Support Programe	4+	22.300 m	TRW/Aerojet	Missile warning
Defense Metereological SP	2	500 m	Lockheed Martin	Nuclear blast det.

Nodos de conexión

- Nodo de College Park, localizado en Maryland-USA
- Nodo de Mountain View, localizado en California-USA
- Nodo de Westminster, en Inglaterra

Estaciones de escucha

Las principales son:

- Morwenstow (Inglaterra), encargada de coordinar las escuchas de satélites INTELSAT en Europa, Océano Atlántico y Océano Pacífico
- Menwith Hill (Inglaterra), para coordinación con satélites diferentes de INTELSAT. Maneja el núcleo central del programa informático
- Bad Aibling (Alemania), para coordinación con satélites diferentes de INTELSAT
- Submarino USS Match, para "pinchar" comunicaciones en cable submarino
- Sugar Grove, en Virginia USA
- Leitrim, Canadá
- Sabana Seca, en Puerto Rico
- Waihopai, Nueva Zelanda
- Shoal Bay, Australia

Otras estaciones y la localización geográfica conocida por reportes diferentes es la siguiente:

- **Yakima (Estados Unidos) 120ºO, 46ºN**

Base del 544º Grupo de Inteligencia (Destacamento 4) de la Air Inteligence Agency (AIA) y del Naval Security Group (NAVSECGRU). Tiene 6 antenas de satélite orientadas hacia los satélites Intelsat del Pacífico y Atlántico. Una de las antenas 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).

- **Sugar Grove (Estados Unidos) 80ºO, 39ºN**

En esta base se encuentra el NAVSECGRU y el 544º Grupo de la AIA (Destacamento 3). Cuenta con 10 antenas de satélite. Tres de ellas serían mayores de 18 metros.

- **Buckley Field (Estados Unidos) 104ºO, 40ºN**

Dirigida por el 544º IG (destacamento 45). Tiene al menos 6 antenas de las cuales cuatro superan los 20 metros. Su cometido es 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.

- **Medina Annex (Estados Unidos) 98º O, 29º N**

RSOC (Centro de Operaciones de Seguridad Regional) controlado por el NAVSECGRU y la AIA, cuya área de acción es el Caribe.

- **Fort Gordon 81º O, 31º N**

RSOC gestionado por el INSCOM y la AIA (702º IG, 721º IG, 202º IB, 31º IS). Sus cometidos son desconocidos.

- **Fort Meade (Estados Unidos)76º O, 39º N**

Sede de la NSA (Agencia de Seguridad Nacional de los Estados Unidos).

- **Kunia (Hawai, Estados Unidos) 158º O, 21º 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 su cometido no está nada claro.

- **Leitrim (Canadá) 75º O, 45º N**

Forma parte de un intercambio de unidades entre Estados Unidos y Canadá. Consta de 4 antenas y las dos mayores son de unos 12 metros de diámetro. Oficialmente esta estación se dedica a la "calificación criptográfica" y a la interceptación de comunicaciones diplomáticas.

- **Sabana Seca (Puerto Rico) 66º O, 18º N**

Utilizada por el Destacamento 2 del 544º 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 de los COMSAT. Se supone que se convierta en la más importante estación de análisis y procesado de comunicaciones por satélite.

- **Morwenstow (Inglaterra) 4º O, 51º 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 no cabe duda de que se dedica a la interceptación de comunicaciones por satélite.

- **Menwith Hill (Inglaterra) 2º O, 53º N**

Utilizada conjuntamente por Estados Unidos y Gran Bretaña. Por parte de los primeros, se encuentran en la estación el NAVSECGRU, la AIA (45º 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.

- **Bad Aibling (Alemania) 12º E, 47º N**

Controlada por el NAVSECGRU, el INSCOM (66º IG, 718 IG) y varios grupos de la AIA (402º IG, 26º 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".

Oficiosamente, 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 decidió cerrar esta estación el 30 de Septiembre del 2002.

- **Agios Nikolaos (Chipre) 32º E, 35º 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.

- **Geraldton (Australia) 114º E, 28º 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.

- **Pipe Gap (Australia) 133º E, 23º 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 de satélite 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.

- **Shoal Bay (Australia) 134º E, 13º 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.

- **Guam (Pacífico Sur) 144º E, 13º S**

Controlada por la 544º 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.

- **Waihopai (Nueva Zelanda) 173º E, 41º 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).

- **Hong Kong 22º N, 114º 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, Misawa, ...). Parece ser que dichas labores se repartieron entre varias estaciones.

- **Misawa (Japón) 141º E, 40º 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.

Programas Robotizados

INTERNET y particularmente los datos y mensajes que circulan por el ciberespacio, se ha convertido en uno de los objetivos de Echelon en los últimos años. Para espiar esta información utilizan programas

informáticos robotizados, los cuales recogen información y ficheros de acuerdo a parámetros pre-seleccionados a lo largo de las Web, los servidores, los portales y las bases de datos.

Software con trampa y software especializado

Hay razonables sospechas de que software de Microsoft, Netscape y Lotus que se exporta de USA, está especialmente adaptado para facilitar la decodificación por parte de la NSA.
Según Margaret Newsham hay dos programas de software conocidos como SILKWORTH y SIRE, especialmente diseñados para Echelon. La red igualmente utiliza sistemas muy desarrollados para reconocimiento de voz (AVR) y reconocimiento de caracteres ópticos (OCR). El sistema central de la red UKUSA se denomina "Platform".

Carnivore (DCS-1000) es la denominación actual y desde 1999, de un software creado en 1997 por Ingenieros de desarrollo del FBI. Fue denominado inicialmente **Omnivore** y construido con el objetivo de intervenir las comunicaciones de INTERNET emulando una intervención telefónica.

Carnivore es un "sniffer" creado para no tener límites de capacidad y opera de esta forma. Aunque no se conoce mucho de él, fue creado como una "caja negra" que recoge toda la información deseable. El FBI lo instala directamente en los ISP (proveedores de servicios de INTERNET), servidores que todos utilizamos para lograr la conexión de red. Toda acción que realizamos por la red es recogida por el ISP. Además del software el FBI instala un hardware compuesto por un PC en una caja modelo rack que se incorpora en las redes de los ISP. De esta manera se asegura poseer toda la información que se desee.

Recientemente la CIA ha construido una herramienta se software que desarrolla actividades parecidas a Echelon. El FBI utiliza también el NetBus, un virus troyano muy poderoso para rastrear comunicaciones y acceder a programas y archivos informáticos.

Se sabe también que el FBI ha estado desarrollando un nuevo troyano denominado Linterna Mágica, con el apoyo de empresas como Symantec (NORTON) y McCaffe para su verificación.

Dentro de Menwith Hill fueron construidos 8 grandes sistemas de comunicación satelital así:

- STEEPLEBUSH. Concluído en 1984
- RUNWAY, para recibir mensajes de satélites Vortex geoestacionarios de segunda generación
- PUSHER, un sistema HFDF que cubre frecuencias HF entre 3-30 Mhz
- MOONPENNY, para los satélites Intelsat
- KNOBSTICKS I and II, para tráfico militar y diplomático
- GT-6, instalado en 1996 para recibir señales de satélites geosincrónicos Advance Vortex y advanced Orion
- STEEPLEBUSH II, para procesar información colectada por RUNWAY
- SILKWORTH, construído por Lockheed Corp. Como el principal sistema de computadores de Menwith Hill

Diccionarios

Constituidos por un sistema especial de ordenadores que encuentran la información deseada utilizando palabras clave, direcciones o áreas de información.

3. Intercepción de Comunicaciones y papel de la red Echelon

Esta compleja infraestructura funciona con base en la escucha de las comunicaciones por medio de "sniffers" y su posterior filtrado. El filtrado se centra en la identificación de palabras clave previamente fijada en grandes diccionarios. Las palabras pueden pertenecer a textos o a voces reales y ser pronunciadas o escritas en diferentes idiomas.

El sistema posee potentes "olfateadores" y programas de reconocimiento de voz. Puede filtran hasta 3.000 millones de mensajes en un ahora.

3.1. ¿Qué tipo de comunicaciones son objeto de interceptación?

Las transmisiones por cable como voz, fax, correo electrónico y datos, sólo se pueden interceptar con acceso físico al cable. Usualmente el proceso se realiza en uno de los extremos del cable y dentro de la jurisdicción de quién ordena la interceptación. Pero también se pueden realizar en 'territorio de nadie", por ej. en la mitad del Atlántico o en territorio extranjero.

Cuando los cables tienen estaciones, como las de amplificación de señal, en estas estaciones también es posible realizar la interceptación. Es el caso de los cables co-axiales que unen Europa con USA que tienen estaciones amplificadoras intermedias.

Utilizando corrientes inductivas es posible interceptar un cable sin necesidad de actuar directamente sobre él, de manera que es posible 'ínterceptar" en cualquier punto si se tiene la tecnología adecuada.

Los cables de fibra óptica de primera generación también se pueden interceptar por medio de corrientes inductivas aplicadas a los amplificadores intermedios, convirtiendo la señal óptica en eléctrica y nuevamente en óptica. Cables ópticos de nueva generación son prácticamente imposibles de interceptar por el alto volumen de datos y las velocidades a que se transportan.

Se deduce que este tipo de interceptación sólo es posible o económicamente factible si se realiza desde los extremos.

La interceptación de las comunicaciones vía INTERNET se facilita hoy día por el hecho de que a diferencia del inicio cuando la red era troncal y el camino del mensaje era según la saturación de la red, hay proveedores del servicio en cantidad, nodos intermedios y "enrutadores" o "encaminadores" de los mensajes. En estos puntos, en donde están localizados estos "routers" se puede realizar la interceptación.

La interceptación de las comunicaciones vía ondas electromagnéticas depende del alcance y tipo de onda empleada. Se debe especificar si son ondas terrestres (las que se mueven por la superficie del planeta) cuyo alcance es limitado y depende de la topografía del terreno, o de ondas indirectas o del espacio (enviadas hacia el espacio y rebotadas en la ionosfera), que generalmente son de gran alcance (ver tabla 2).

Tabla 2. Ondas electromagnéticas

LONGITUD	TIPO	CARACTERISTICAS
Larga (3-300 kHz)	Terrestre	No se reflejan. Alcance corto
Media (300kHz-3MHz)	Terrestre	Se reflejan de noche. Alcance medio
Corta (3-30MHz)	Indirecta	Se reflejan, reflexión múltiple, cobertura mundial absoluta
Ultracorta (30-300MHz)	Terrestre	No se reflejan, difusión rectilínea, alcance limitado según curvatura del planeta, orografía, altura de antenas y potencia de transmisión. Alcance de hasta 100 Km. Los móviles se reducen a 3º Km.
Decimétricas y Centimétricas (300MHz-30GHz)	Terrestre	Muy rectilíneas. Se pueden separar en haces. Adquieren gran precisión y poca potencia de transmisión. Se

		captan con antenas cercanas, paralelas al haz de transmisión o dentro de él en su prolongación

Las ondas largas y medias se utilizan para transmisiones radiofónicas, de radiobalizas, etc. La comunicación militar y civil se realiza por onda corta, ultracorta, decimétrica y centimétrica, de manera que su interceptación debe realizarse como máximo a 100 Km. del punto espiado y suele realizarse desde aviones, navíos y embajadas.

Otro tipo de transmisiones es la que corresponde a los satélites geoestacionarios, aparatos que pueden recibir y enviar señales a grandes distancias, aunque no desde cualquier parte del mundo, salvo que hagan parte de un sistema o grupo de satélites. Las estaciones de escucha se localizan generalmente en zonas puntuales, de manera que pueden ejecutar con gran eficiencia la interceptación de fax, teléfono y datos.

Tabla 3. Sistemas internacionales de satélites

SISTEMA	SATELITES	COBERTURA	PAISES
INTELSAT	20	Atlántico, Indico y Pacífico.	200
INTERSPUTNIK	4	Mundial	40
INMARSAT	9	Intercomunicación de vehículos marítimos, aéreos y terrestres	Mundial
EUTELSAT	18	Europa, Asia y Africa. Algo de América	40
ARABSAT	1	Zona árabe	Países árabes
PALAPA	1	Asia Meridional	12
TELECOM	1	Francia, Africa y Suramérica	Francia y Dptos. Ultramar
AMOS	1	Medio Oriente	Israel y medio oriente
HISPASAT	1	España y Portugal. TV para América	15
PANAMSAT	21	USA y América. Algo Europa	40
ITALSAT	1	Italia	1

De acuerdo con lo anterior, los mensajes que se interceptan pueden ser llamadas telefónicas, correos electrónicos, archivos descargados de INTERNET, transmisiones satelitales, comunicaciones de fax y otras.

Operativamente, primero se definen las palabras clave, en varios idiomas y con base en ellas se filtran u olfatean las comunicaciones, incluyendo las de INTERNET sobre las que se asume hay una captación del 90%, dado que todo el flujo de esta red pasa por los NODOS de USA y por 9 puntos de control de la NSA.

Una vez que se detecta una comunicación de "interés", el sistema informático inicia su monitoreo y grabado. Se etiqueta y envía a los centros de análisis. Dependiendo del origen y la fecha se marca con un número clave. Se transcribe, descifra, traduce y se guarda como un informe más o menos extenso.

Los informes se codifican según el nivel de secreto que se le otorgue como: "Morai" o secreto; "Spoke" o más secreto; "Umbra" o alto secreto; "Gamma" o comunicaciones rusas; " Druid" informe para países no miembros de la red.

Tabla 4. Códigos, agencias y países

CODIGO	AGENCIA	PAIS
Alpha	GCHQ	Gran Bretaña
Echo	DSD	Australia
India	GCSB	Nueva Zelanda
Uniform	CSE	Canadá
Oscar	NSA	Estados Unidos

Si se considera que una transmisión es peligrosa para los países miembros de Echelon, quienes participen en ella pasan a hacer parte de una "lista negra" y sus comunicaciones y acciones son espiadas a partir de entonces.

4. Los Diccionarios de Echelon

Una de las características de Echelon es su capacidad de interceptar la mayor parte de las comunicaciones del mundo. No sólo intercepta, también des-encripta, filtra, examina y codifica esta información. Todas las señales electrónicas son llevadas a la estación de Menwith Hill, donde se vierten en grandes sistemas de computadores dentro de los cuales se analizan con dispositivos para reconocer voces, para reconocer caracteres ópticos y para análisis informático.[11]

Se afirma que los programas de computador que utilizan trascienden "el estado del arte" o son parte del futuro en este campo. Parte del sistema de super-computadores de Menwith Hill se conoce como MAGISTRAND y contiene los más poderosos programas para investigar "keywords".

Se conoce también una herramienta manufacturada por MEMEX (compañía británica), denominada PATHFINDER que recorre los mensajes y sus "footnotes" a través de palabras clave y frases basadas en complejos algorítmicos.

Los programas de reconocimiento de voz convierten las conversaciones en mensajes de texto para el posterior análisis. El extraoficialmente conocido como VOICECAST, puede identificar un patrón individual de voz y archivarlo para uso posterior.

Echelon procesa millones de mensajes cada hora, durante las 24 horas del día, siete días a la semana, a través de series de "keywords", de números de fax y teléfonos y de patrones de voz específicos. Todo indica que en la actualidad, relativamente pocos son los mensajes y las llamadas telefónicas que se trascriben y registran. La mayoría son eliminados después de ser leídos por el sistema.[12]

Cada nodo o estación de Echelon maneja una lista de "keywords". Estas listas son los **diccionarios.** Las listas son elaboradas por las agencias de inteligencia de los países participantes en la red. Cada agencia tiene un "manejador o gerente del diccionario", quien es el responsable de adicionar, borrar o cambiar las palabras clave del respectivo diccionario. Para cada estación hay "códigos", como p.ej. COWBOY para Yakima ó FLINTLOCK para Waihopai. Estos códigos juegan un papel crucial en el análisis y procesamiento de los mensajes.

Tal y como está organizada la red, ésta no permite que p. ej. las autoridades neozelandesas puedan conocer los

[11] POOLE, Patrick S. (2000). *ECHELON: America`s Secret Global Surveillance Network.* En: http://fly.hiwaay.net/~pspoole/echelon.html

[12] op. Cit.

diccionarios utilizados por UKUSA, si bien lo contrario es posible.[13]

Cada mensaje escogido por los diccionarios de Echelon es "identificado" por un código de cuatro dígitos que representa el origen o el sujeto. Por ej. 5535 para tráfico diplomático japonés o, 8182 para comunicaciones acerca de la distribución de tecnología de encriptación.

La "identificación" también incluye el código de las agencias: ALPHA-ALPHA (GCHQ), ECHO-ECHO (DSD, INDIA-INDIA (GCSB), UNIFORM-UNIFORM (CSE) y OSCAR-OSCAR (NSA).

Los mensajes identificados son transmitidos por el sistema global de computadores PLATFORM a cada agencia. PLATFORM actúa como el sistema nervioso informático para las estaciones UKUSA y las agencias.

Los análisis diarios de los mensajes que realiza cada agencia, pueden ser compilados en: reportes. Estos reportes se categorizan según el grado de "secreto" que se les asigne.

5. Información y política

Una visión global de la concepción u origen, la estructura y la forma de operación de la red Echelon, permite concluir que hay una motivación político-militar en ella. Se puede aventurar como hipótesis que esta motivación ha ido cambiando con el tiempo, sin perder su condición esencial.

En 1948 las necesidades de información se basaban en la condición bélica (político-militar)) de la II Guerra Mundial. La necesidad era la información para los países aliados. Pero en la década de los años 70, durante la Guerra Fría entre las dos superpotencias y sus respectivos bloques, la motivación político-militar fue la información para sacar ventajas estratégicas en la confrontación entre estos dos polos.

Concluida la Guerra Fría, la motivación político-militar toma diferentes contenidos: primero la "seguridad nacional" de USA y los miembros de la red; luego, la "lucha contra el terrorismo y el tráfico de drogas" y finalmente? Todo indica que la motivación político-militar ahora se refiere a la necesidad de lograr una "hegemonía" de poder sobre el mundo, pero matizada con la respuesta a intereses de tipo industrial y económico.

¿Coincide la motivación político-militar y comercial de Echelon a los nuevos tiempos? La respuesta es sí. En tiempos de globalización, particularmente por los efectos geopolíticos que ella produce, la información es esencial para la consolidación de una forma de soberanía imperial y de un mercado global dominado por los conglomerados económicos de propiedad de USA y sus aliados.

El agotamiento de las "soberanías nacionales", incluso los problemas de las instituciones creadas por la interacción de los estados nacionales a través del Derecho Internacional, como por ejemplo la ONU, es correspondiente a la tendencia creciente de consolidación de una nueva forma de soberanía, el imperio.[14]

Esta forma de soberanía para consolidarse como un gobierno mundial requiere tener el control de las comunicaciones. Para ello se ha desarrollado un proyecto como Echelon.

Dado que esta tendencia está representada no sólo por UKUSA, también hay otros países o alianzas que han desarrollado proyectos de espionaje de las comunicaciones. Sin embargo, Echelon se muestra como la más efectiva, compleja y completa.

---

[13] VARIOS AUTORES. (2002). *La gran oreja: red de satélites espía de la US National Security Agency (NSA). Países anglosajones espían Europa.* En http://www.enlaces

[14] NEGRI, Tony y Richard Hardt. (2000). *Imperio*. Harvard University Press. Massachussets. USA

5.1 Espionaje doméstico y político

El espionaje que se adelanta a través de Echelon parece no tener límites. Ciudadanos de USA han sido objeto de hostigamientos y espionaje de tiempo atrás, pero con Echelon las cosas han tomado otros contenidos, de manera que para burlar la legislación propia, que prohíbe constitucionalmente tales prácticas, la NSA orienta las acciones de espionaje con otras agencias de la red.

Los sucesos del 11 de septiembre igualmente están siendo la base para modificar la legislación norteamericana y a través de sus dictados, la de otros países. Pero de igual forma, la globalización de la vida humana en todos sus aspectos ha venido exigiendo cambios en esta legislación, particularmente la que se basa en la noción de **seguridad nacional.** Lo que se observa es que ésta se modifica para incluirle los aspectos concernientes a lo comercial, lo económico y lo corporativo.

En USA desde que fue creada la NSA por el presidente Truman, esta agencia u otras relacionadas, ha sido utilizada para el espionaje doméstico y político. De esta historia patética se conocen varios proyectos:

- Proyecto SHAMROCK

Este proyecto se inició en 1945 con la misión de obtener copias de la información telegráfica existente en USA o que entraba a esa unión. En el cometido contó con la colaboración de la RCA, la ITT y la Western Union.

El sistema inicial de microfilmación cambió radicalmente con el uso de cintas magnéticas de computador, a través del famoso HARVEST que tenía la capacidad de gravar las comunicaciones y espiarlas a través de palabras clave, localizaciones, remitentes y direcciones.

El proyecto fue tan exitoso que en 1966 la NSA y la CIA, crearon una compañía en el bajo Manhattan, con el código de LPMEDLEY, a través de la cual los propios agentes de espionaje, en un mes, imprimieron y analizaron 150.000 mensajes recopilados por SHAMROCK.

El proyecto fue finalmente desmontado en mayo de 1975 después de ser cuestionado por el Congreso norteamericano.

- Proyecto MINARET

Es un proyecto gemelo del SHAMROCK, pero fue la base para crear las "listas de observación" que el FBI utilizó para sindicar de "subversivas" muchas actividades domésticas. Estas listas incluyeron nombres como los de Martin Luther King, Malcolm X, Jane Fonda, Joan Baez y el Dr. Benjamín Spock. Operó entre 1967 y 1973 sobre 5925 extranjeros y 1690 organizaciones y ciudadanos norteamericanos. La NSA mantuvo reportes sobre 75000 ciudadanos americanos entre 1952 y 1974.

- Operación CHAOS

En forma paralela a los proyectos HAMROCK y MINARET, por orden del presidente Lyndon Jonson, la CIA creó la DOD (Domestic Operation Division), cuyo propósito era "dirigir, soportar y coordinar operaciones clandestinas contra activistas dentro de USA".

Frente a las crecientes protestas estudiantiles por la guerra de Vietnam, la DOD creó dos unidades de acción contra las organizaciones y los activistas anti-guerra: el proyecto RESISTANCE y el proyecto MERRIMAC. El primero se desarrolló en coordinación con los directores de los College y las Universidades, la seguridad de los campus y las policías locales. El segundo monitoreaba cualquier demostración anti-guerra en Washington.

El presidente Nixon oficializó todas estas actividades de vigilancia doméstica en la Operación CHAOS. El proyecto murió después de las revelaciones sobre el escándalo Watergate y la publicación en el New York

Times sobre los abusos de la CIA en la vigilancia de ciudadanos norteamericanos.

Durante su existencia, investigaciones del Senado revelaron que la CIA había elaborado 13000 informes individuales sobre actividades disidentes, incluyendo 7000 de ciudadanos norteamericanos y 1000 organizaciones.

- The Foreign Intelligence Surveillance Court (FISC)

El Congreso de USA creó la FISC como una corte "top-secret" para enterarse de las aplicaciones de vigilancia electrónica que realizaba el FBI y la NSA, y para chequear las actividades domésticas de estas agencias. Esta corte se establece como un "perro guardian" de los derechos constitucionales del pueblo americano, con un perfil de defensa frente a los abusos de las actividades del FBI y la NSA.

Se conocen intentos documentados sobre la utilización de Echelon con fines de espionaje político. Un episodio describe la orden de Margaret Thatcher, en 1988, para espiar a dos ministros de su gabinete, sospechosos de deslealtad. Otro se refiere al espionaje de que fue objeto el primer ministro Pierre Trudeau y su esposa. En el primer caso estuvieron involucradas las agencias norteamericanas e inglesas (UKUSA) y en el segundo el servicio secreto de la Real Policía Montada Canadiense.

5.2 Espionaje comercial, industrial y tecnológico

Varios estudiosos coinciden en afirmar que "con la rápida erosión del imperio soviético al inicio de los años 90, las agencias de inteligencia occidentales se apresuraron a redefinir sus misiones para justificar el espectro del sistema de vigilancia global"[15] Producto de ello es la redefinición de la noción de "seguridad nacional" para poder incluir actividades de espionaje sobre competidores de prominentes Corporaciones norteamericanas.

Evidentemente no todo el espionaje comercial se inició entonces. Ya desde 1970, Gerald Burke, director ejecutivo de la FIAB ( )[16] bajo la orden del Presidente Nixon, reconoció haber realizado actividades de espionaje comercial como una función de seguridad nacional con una prioridad equivalente a la inteligencia diplomática, militar o tecnológica.

Desde muy temprano en la década de los 90, se conocieron las denuncias sobre espionaje comercial a través de gobiernos o medios de comunicación.

- *Der Spiegel* reveló que la NSA en 1990, había interceptado mensajes sobre la negociación Indonesia-Japón (NEC) para la manufactura de un satélite por valor de 200 millones de dólares. Por intervención del Presidente Bush (padre) el negocio fue asignado a ITT+NEC.
- En 1994, la CIA y la NSA interceptaron llamadas telefónicas sobre la negociación entre Brazil y la empresa francesa Thomson-CSF, sobre la negociación de un sistema de radares.
- En septiembre de 1993, el presidente Clinton ordenó a la CIA espiar las fábricas japonesas de autos que habían diseñado motores "cero-emisión" y entregar la información a las tres gigantes norteamericanas del automóvil: Ford, General Motors y Chrysler.
- En 1995 el *New York Times* volvió a denunciar las actividades de espionaje de la CIA y la NSA a favor de USA en las negociaciones en Génova sobre automóviles entre Japón-USA. Recientemente el periódico japonés *Mainichi* acusó a la NSA por continuar las labores de monitoreo de las comunicaciones de compañías japonesas.
- *Insight Magazine* reportó en una serie de artículos en 1977, que el presidente Clinton ordenó a la NSA y al FBI una operación de vigilancia masiva en la Conferencia Económica ASIA/PACIFICO realizada en Seattle en 1993. Igual sucedió con las negociaciones de

[15] op.cit

[16] Citado por POOLE, Patrick S. (2000). *ECHELON: America¨s Secret Global Surveillance Network.* En: http://fly.hiwaay.net/~pspoole/echelon.html

Vietnam para la compra de aviones Boeing.

No sólo USA ha realizado estas actividades. Se tiene conocimiento que también UK y otros países, particularmente los que intervienen en la red Echelon, han realizado este tipo de espionaje, a favor de compañías que fabrican partes para la red.

6. Defensa de la privacidad y la libertad

El derecho a la privacidad y a la libertad de información constituyen dos bienes preciados de la humanidad moderna. Los intentos por vulnerarlos siempre han estado prevenidos en las legislaciones nacionales y en el derecho internacional. Sin embargo, hay múltiples evidencias que demuestran que por encima de las legislaciones se colocan superpoderes que los afectan o que hacen acuerdos para violarlos.

El caso más conocido es el de las libertades civiles en la sociedad norteamericana. Estos derechos contemplados en la Constitución son vulnerados directa o indirectamente por las decisiones político-militares de los gobiernos. Tal vez se pueda decir que ahora, en la sociedad global que funciona en red[17], también se afectan estos derechos por las decisiones económicas y financieras.

El proyecto Echelon y otros proyectos de distintos países son realmente acciones contra el derecho a la privacidad y a la libertad de información. Los mensajes y las informaciones privadas, de personas o de instituciones, son abiertos, analizados y clasificados por quienes ostentan el poder sobre las comunicaciones.

Pero así como hay proyectos y desarrollos tecnológicos en este sentido también los hay en el sentido contrario: la defensa del derecho a la libertad y a la privacidad en la información.

6.1 La ACLU y el surgimiento previsible de la "American Surveillance Society"

Bajo el estigma de que la visión de Orwell sobre el "Gran Hermano" (Big Brother)[18] es por primera vez en la historia de la humanidad, tecnológicamente factible, muchas organizaciones y personas han iniciado movimientos por las libertades civiles y contra un modelo de sociedad imperial totalmente vigilada.

La *American Civil Liberties Union (ACLU)* [19] es una organización que como "primer guardián de la libertad de la nación" trabaja diariamente en las cortes, legislaturas y comunidades para defender y preservar los derechos individuales y las libertades garantizadas por la Constitución y las leyes de USA.

Para la ACLU[20] la explosión de computadores, cámaras, sensores, comunicaciones inalámbricas, GPS, telemetrías y otras tecnologías (reconocimiento de cara con microchips implantables, data-mining, chips de ADN y huellas de hondas cerebrales) que han aparecido en los últimos 10 años, son la base tecnológica para la aparición de una "Surveillance Society" en América. Probablemente el primer paso hacia una sociedad mundial de la misma condición, el famoso "big brother" de George Orwell.

La ACLU observa una pérdida gradual de los derechos de privacidad y libertades civiles, situación que se ha incrementado notablemente después de los actos terroristas del 11 de septiembre de 2001. Estos hechos se han tomado como un pretexto para actuar contra la sociedad civil de manera que no es aventurado ver en el inmediato futuro, escenarios como estos:

- "An African-American man from the central city visits an affluent white suburb to attend a cowork`s barbeque. Lather the nigt, a crime takes place elsewhere in the neighborhood. The police review surveillance camera images, use face recognition to identify the man, and pay

[17] CASTELLS, Manuel. (1999). *La era de la información: economía, sociedad y cultura.* Traducción de Carmen Martínez Gimeno. Siglo XXI Editores. México.
[18] Ver en: http//:www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39
[19] www.aclu.org
[20] ACLU. (2003). Reporte de enero sobre *Bigger Monster, Weaker Chains: the growth o fan American Surveillance Society.* By Jay Stanley and Barry Steinhardt. Programa de Libertad y Tecnología.

him a visit at home the next day. His trip to the suburbs where he "didn´t belong" has earned him an interrogation from suspicious police.

- A tourist walking through an unfamiliar city happens upon a sex shop. She stops to gaze at several curious items in the store´s window before moving along. Unbeknownst to her, the store has set up the newly available "Customer Identification System", which detects a signal being emitted by a computer chip in her driver´s license and records her identity and the date, time, and duration of her brief look inside the window. A week later, she gets a solicitation in the mail mentioning her "visit" and embarrassing her in front of the family."

Estos escenarios son solo la punta del iceberg, pues la nueva legislación sobre interceptación de comunicaciones y espionaje personal pueden ser componentes adicionales de ellos. Se pueden adicionar finalmente, las consecuencias del espionaje electrónico de las comunicaciones para tener un panorama más completo de las situaciones que vendrán para las libertades civiles individuales y sociales.

Esta nueva situación da origen a una base de lucha por las libertades civiles, no sólo en USA sino en cualquier país del mundo.

6.2 Respuesta Europea al espionaje industrial de UKUSA

La reacción de la Unión Europea a la publicación de Duncan Campbell deberá tener desarrollos diferentes a los dos informes mencionados. La Comisión Echelon del Parlamento Europeo, que ha confirmado no solamente la existencia de la red de espionaje sino su intervención en asuntos de espionaje industrial y comercial a favor de corporaciones de los países miembros, seguramente recomendará otro tipo de acciones. No está en juego solamente el problema de la dominación del mercado global, también el problema político de la soberanía de los países europeos y de la presencia regional europea en el mundo.

Es sabido por ejemplo que diferentes países de la UE han desarrollado sus propias redes de interceptación y espionaje de comunicaciones, como:

- Francia con FRANCHELON
- Rusia con SORM
- Suiza con SATOS3

La propia UE aprobó en mayo de 1999 un proyecto de red de espionaje denominado ENFOPOL, cuyo campo de acción se supone limitado a la Unión.

6.3 Encriptación y PGP

Los usuarios de la red INTERNET no deben defenderse solamente de Echelon, también de múltiples clases de software, genéricamente conocido como SPYWARE que son instalados en forma "gratuita" o con el "consentimiento del usuario" en sus propios ordenadores.

El SPYWARE está constituido por archivos o aplicaciones que monitorean y pueden enviar información de las actividades de quienes los tienen instalados.

Al SPYWARE se le suma el software comercial que llega "sin permiso" a los computadores personales. Se le conoce como ADWARE.

Pero, en defensa de la libertad y la privacidad de la información que se cursa por INTERNET, se han desarrollado sistemas de protección de la información como el Pretty Good Privacy o PGP.

Este programa gratuito y de libre distribución es una de las formas más usuales y seguras de encriptación. Se trata de un sistema de doble clave, pública y privada, similar al que se utiliza por ejemplo para encriptar mensajes en Netscape, pero mucho más seguro.

La clave pública, que se utiliza para encriptar los mensajes con PGP, pero que no permite des-encriptarlos,

puede distribuirse a todos los corresponsales, mientras que la clave privada, única que permite des-encriptarlos, sólo se conoce por el propietario y quien deba desencriptar un mensaje específico.

Aunque el PGP está prohibido exportarlo de USA, se puede instalar gratuitamente en la dirección http://www.pgpi.org

La existencia de programas como PGP es vista como una amenaza por las agencias de espionaje y la red Echelon. El gobierno norteamericano ha propuesto incluso una variante del PGP para facilitar la des-encriptación de mensajes que utilicen el sistema.

7. Conclusiones

7.1 Si bien Echelon no es el único sistema de espionaje existente, si constituye el proyecto que ha efectuado mayor número de acciones no legales, evidentes, sobre países y empresas, y tal vez personas, en el transcurso de los últimos años. Todo indica que Echelon es un proyecto esencial en la construcción de una nueva forma de imperio universal basada en el manejo de la información.

7.2 Echelon es un sistema tan real como poderoso, y tan eficaz como desconocido… es un sistema de interceptación, clasificación y evaluación de las telecomunicaciones. Tiene tres características esenciales:

- Es internacional tanto en ámbito como en composición
- Fue diseñado para que se comporte como una entidad inteligente. No se limita a interceptar mensajes y re-transmitirlos
- A diferencia de otros sistemas, Echelon fue diseñado específicamente para captar y procesar grandes cantidades de información en redes de transmisión CIVILES

7.2 Puede definirse como un "conglomerado político-económico al servicio de determinado trust, ya que proporciona la información suficiente y necesaria para que las compañías norteamericanas tengan un control absoluto de los negocios del mundo y la información política para que USA tome las medidas que considere necesarias para mantener su dominación mundial.

7.3 Echelon es un término inglés que significa "escalón", aunque esta red también es conocida como "la gran oreja". Como tal es un programa informático, pero como red es un entramado de antenas, estaciones de escucha, radares, satélites, submarinos y aviones espía, unidos todos estos elementos a través de bases terrestres, cuyo objetivo es espiar las comunicaciones mundiales, teóricamente para la lucha contra el terrorismo internacional y el tráfico de drogas.

7.4 Su compleja infraestructura funciona con base en la escucha de las comunicaciones por medio de "sniffers" y su posterior filtrado. El filtrado se centra en la identificación de palabras clave previamente fijada en grandes diccionarios. Las palabras pueden pertenecer a textos o a voces reales y ser pronunciadas o escritas en diferentes idiomas.

7.5 El sistema posee potentes "olfateadores" y programas de reconocimiento de voz. Puede filtran hasta 3.000 millones de mensajes en un ahora.

7.6 La interceptación de las comunicaciones vía INTERNET se facilita hoy día por el hecho de que a diferencia del inicio cuando la red era troncal y el camino del mensaje era según la saturación de la red, hay proveedores del servicio (ISP) en cantidad, nodos intermedios y "enrutadores" o "encaminadores" de los mensajes. En estos puntos, en donde están localizados estos "routers" se puede realizar la interceptación.

7.7 Una de las características de Echelon es su capacidad de interceptar la mayor parte de las comunicaciones del mundo. No sólo intercepta, también des-encripta, filtra, examina y codifica esta información. Todas las señales electrónicas son llevadas a la estación de Menwith Hill, donde se vierten en grandes sistemas de computadores dentro de los cuales se analizan con dispositivos para reconocer voces, para reconocer caracteres ópticos y para análisis informático

7.8 Echelon procesa millones de mensajes cada hora, durante las 24 horas del día, siete días a la semana, a través de series de "keywords", de números de fax y teléfonos y de patrones de voz específicos. Todo indica que en la actualidad, relativamente pocos son los mensajes y las llamadas telefónicas que se trascriben y registran. La mayoría son eliminados después de ser leídos por el sistema

7.9 Una visión global de la concepción u origen, la estructura y la forma de operación de la red Echelon, permite concluir que hay una motivación político-militar en ella. Se puede aventurar como hipótesis que esta motivación ha ido cambiando con el tiempo, sin perder su condición esencial, así:

- En 1948 las necesidades de información se basaban en la condición bélica (político-militar)) de la II Guerra Mundial. La necesidad era la información para los países aliados.
- En la década de los años 70, durante la Guerra Fría entre las dos superpotencias y sus respectivos bloques, la motivación político-militar fue la información para sacar ventajas estratégicas en la confrontación entre estos dos polos.
- Concluida la Guerra Fría, la motivación político-militar toma diferentes contenidos: primero la "seguridad nacional" de USA y los miembros de la red; luego, la "lucha contra el terrorismo y el tráfico de drogas" y finalmente? Todo indica que la motivación político-militar ahora se refiere a la necesidad de lograr una "hegemonía" de poder sobre el mundo, pero matizada con la respuesta a intereses de tipo industrial y económico.

7.10 No sólo USA ha realizado estas actividades. Se tiene conocimiento que también UK y otros países, dentro y fuera de la red Echelon, han realizado este tipo de espionaje, a favor de compañías que fabrican partes para la red.

7.11 El derecho a la privacidad y a la libertad de información constituyen dos bienes preciados de la humanidad moderna. Los intentos por vulnerarlos siempre han estado prevenidos en las legislaciones nacionales y en el derecho internacional. Sin embargo, hay múltiples evidencias que demuestran que por encima de las legislaciones se colocan superpoderes que los afectan o que hacen acuerdos para violarlos.

7.12 El proyecto Echelon y otros proyectos de distintos países son realmente acciones contra el derecho a la privacidad y a la libertad de información. Los mensajes y las informaciones privadas, de personas o de instituciones, son abiertos, analizados y clasificados por quienes ostentan el poder sobre las comunicaciones.

7.13 Los usuarios de la red INTERNET no deben defenderse solamente de Echelon, también de múltiples clases de software, genéricamente conocido como SPYWARE que son instalados en forma "gratuita" o con el "consentimiento del usuario" en sus propios ordenadores.

7.14 En defensa de la libertad y la privacidad de la información que se cursa por INTERNET, se han desarrollado sistemas de protección de la información como el Pretty Good Privacy o PGP.

Este programa gratuito y de libre distribución es una de las formas más usuales y seguras de encriptación. Se trata de un sistema de doble clave, pública y privada, similar al que se utiliza por ejemplo para encriptar mensajes en Netscape, pero mucho más seguro.

8. Bibliografía

ACLU. (2003). *Echelon counterparts. Last updated or verified on February 5/2003.* En:
ACLU. (2003). *Echelon watch.* En: http://www.echelonwatch.org/
ACLU. (2003). Reporte de enero sobre *Bigger Monster, Weaker Chains: the growth o fan American Surveillance Society.* By Jay Stanley and Barry Steinhardt. Programa de Libertad y Tecnología.
BLADET, Ekstra. (1999). *Echelon.* Entrevistas con Margareth Newsham ex-agente de la NSA en Echelon. Traducido por Wintermute.

CAMPBELL, Duncan. (1988). *Alguien está escuchando.* New Statesman, 12 de agosto. En: http://jya.com/echelon-dchtm
CAMPBELL, Duncan. (1999). *Interception capabilities 2000.* En: http://www.iptvreports.mcmail.com/stoa_cover.html
CASTELLS, Manuel. (1999). *La era de la información: economía, sociedad y cultura.* Traducción de Carmen Martínez Gimeno. Siglo XXI Editores. México.GPO/ Bogotá, Colombia, abril 26 de 2003
DELGADO, Javier. (2001). *La privacidad en el ciberespacio.* ARTICULO. (2001). *¿Qué es el proyecto Echelon?*
HERNANDEZ, Jorge. (2001). *Echelon – El espía 415.* EL ESPECTADOR. Bogotá Colombia. Mayo. RedRoj@. (2000). *Contra Echelon, PGP.*
http://archive.aclu.org/echelonwatch/networks.html
JAY, Stanley and Barry Steinhardt. (2003). *Bigger Monster, weaker chains: the growth of an American Surveillance Society. Jasnuary 15.* En: http://www.aclu.org/news/Newsprint.cfm?ID=11573&c=39
NEGRI, Tony y Richard Hardt. (2000). *Imperio*. Harvard University Press. Massachussets. USA
OLIVERAS, Eliseo y Antonio Fernandez. (2001). *La traición de Londres: nuestros socios y aliados nos espían.* En http://www.tiempodehoy.com
POOLE, Patrick S. (2000). *ECHELON: America¨s Secret Global Surveillance Network.* En: http://fly.hiwaay.net/~pspoole/echelon.html
POOLE, Patrick S. (2000). *ECHELON: America¨s Secret Global Surveillance Network.* En: http://fly.hiwaay.net/~pspoole/echelon.html
QUIRANTES, Arturo. (2001). *Echelon: vigía del imperio*. En aquiran@goliat.ugr.es
VARIOS AUTORES. (2002). *La gran oreja: red de satélites espía de la US National Security Agency (NSA). Países anglosajones espían Europa.* En http://www.enlaces
VINDREM, Robert. (1998). *Spy satellites enter new dimension.* MSNBC y NBC News, August 8
WRIGHT, Steve. (1988). *An appraisal of technologies for political control.* En: http://cryptome.org/stoa-atpc.htm