Llega un nuevo software espía

Debuta la Vigilancia en una caja

09/09/2008 - Autor: Tom Burghardt (Global Research) - Fuente: Rebelión

Habréis oído hablar del “Circuito Cuántico” del FBI y os indignaron las escuchas ilegales sin mandato judicial de los acólitos de Bush. No sirvieron para nada los correos y llamados telefónicos con los que inundasteis el Congreso, enfurecidos por la bipartidaria “Ley de Enmiendas a FISA de 2008.” y por la elegantísima fiesta lanzada por AT&T para los demócratas “Blue Dog” La Coalición del Perro Azul, conservadores con base rural y sureña, aliados ocasionales de los republicanos en Denver esta semana con motivo de la convención.

Pero justo a tiempo para un nuevo gobierno (y los montones de dinero siempre disponible para el creciente mercado interno de la seguridad), llega un completo sistema de “vigilancia en una caja” llamado Plataforma de Inteligencia.

Según New Scientist, el gigante alemán de la electrónica, Siemens, ha desarrollado software que supuestamente es capaz de integrar:

tareas realizadas típicamente por equipos o dispositivos separados de vigilancia, combinando datos de fuentes como ser llamados telefónicos, actividad de correo electrónico e Internet, transacciones bancarias y cuentas de seguros. Luego analiza esa montaña de información utilizando software que Siemens apoda “módulos de inteligencia.” (Laura Margottini, "Surveillance Made Easy," New Scientist, 23 de agosto de 2008)

New Scientist informa que la firma ha vendido el sistema a unos 60 países en Europa y Asia. ¿Qué países? Bueno, Siemens no lo revela.

Sin embargo, defensores de la privacidad y de los derechos humanos dicen que el sistema tiene un notable parecido con el “Escudo Dorado” de China, una masiva red de vigilancia que integra inmensas bases de datos, monitoreo de Internet y de correos electrónicos, plataformas de reconocimiento facial y verbal en combinación con control por CCTV (circuitos cerrados de televisión).

Diseñada especialmente para “centros de fusión” o sus equivalentes europeos/asiáticos, la Plataforma de Inteligencia promete suministrar instrumentos de alta tecnología en “tiempo real” para frustrar complots terroristas antes de que sean tramados (o controlar a activistas contra la globalización o contra la guerra).

El último ítem en el mercado emergente del nicho en el mercado del software “inteligente”, Plataforma de Inteligencia ha sido “entrenado” en una gran cantidad de documentos utilizados como muestra para centrarse en nombres, números de teléfono o sitios de texto genérico. “Esto significa que puede identificar nombres o números que aparecen junto a cualquiera que sea de interés para las autoridades, y luego catalogar todos los documentos

que contengan esas asociaciones," afirma New Scientist.

En el Reino Unido, el Home Office (Ministerio del Interior) anunció que planifica suministrar acceso a los detalles de mensajes de texto, correos electrónicos y búsquedas en Internet a agencias de mantenimiento del orden, consejos locales y otras agencias públicas. Esto viene inmediatamente después de un anuncio en mayo pasado de que el Nuevo Laborismo está considerando la formación de una masiva base centralizada de datos "como instrumento para ayudar a que los servicios de seguridad hagan frente al crimen y al terrorismo." Según The Guardian:

consejos locales, autoridades sanitarias y cientos de otros organismos públicos recibirán derecho de acceder a detalles de textos personales, correos electrónicos y uso de Internet de todos, según propuestas del Home Office publicadas ayer.

Los ministros quieren hacer que compañías telefónicas y de Internet sean obligadas a mantener detalles de todo el tráfico personal por Internet durante por lo menos 12 meses para que se pueda tener acceso para investigaciones de crímenes o de otras amenazas para la seguridad pública...

Los conservadores y los demócratas liberales calificaron anoche esta medida como una "carta de privilegios para fisgones". (Alan Travis, "Snoopers charter to check texts and email," The Guardian, miércoles 13 de agosto de 2008)

Una publicidad colocada en el sitio en la Red de Siemens afirma que el "desafío" es "promover el bienestar de ciudadanos respetuosos de la ley" y que por ello, "grupos autorizados tienen que tener acceso directo a comunicaciones entre sospechosos, sean individuos, grupos u organizaciones. Sólo entonces podrán emprender la acción apropiada: detectar, impedir y anticipar crímenes y garantizar la paz y la seguridad."

En otras palabras, si no tenéis nada que ocultar, "confiad en nosotros:" el gastado mantra de securócratas por doquier. Y en el clima actual, es un desafío especialmente agobiante para la seguridad estatal y los espías corporativos que exigen "grabaciones altamente sofisticadas, multiniveles, de voz y datos" a fin de destruir nuestros derechos mientras transforman nuestras respectivas sociedades en Estados policiales orwellianos. El New Scientist informa:

Una vez que una persona esté siendo controlada, software de reconocimiento de modelos identifica primero su conducta típica, como ser llamados repetidos a ciertos números durante un período de unos pocos meses. El software luego identifica toda desviación de la norma y marca actividades inusuales, como ser transacciones con un banco extranjero, o contacto con alguien que también esté bajo vigilancia, para que los analistas puedan examinarlo de más cerca.

Pero si la experiencia de los Centros de Fusión de EE.UU. han de dar alguna idea de la exactitud del sistema de Siemens, los positivos falsos serán endémicos mientras miles, si no millones, de individuos perfectamente inocentes son atrapados para siempre en la traína de datos del Estado. Según la Unión Estadounidense para las Libertades Civiles:

Las líneas directivas del Departamento de Justicia prevén que los centros de fusión hagan más que simplemente compartir información legítimamente adquirida de mantenimiento del orden a través de diversas ramas de nuestro floreciente establishment de la seguridad. Las

Líneas Directivas exhortan a recopilar datos "de fuentes no-tradicionales, como ser entidades de seguridad pública y organizaciones del sector privado" y aliarlas con inteligencia federal "para anticipar, identificar, prevenir y/o controlar actividad criminal y terrorista." Esto implica el uso considerable de traínas estadísticas que han llegado a ser llamadas minería de datos. El resultado inevitable de un enfoque de minería de datos será que:

Numerosos individuos inocentes serán marcados, escrutados, investigados, colocados en listas de vigilancia, interrogados o arrestados, y posiblemente sufran un daño irreparable a su reputación, todo debido a una maquinaria oculta de intermediarios de datos, distribuidores de información y algoritmos informáticos.

Las agencias de cumplimiento de la ley desperdiciarán tiempo y recursos invirtiendo en chatarra informática de alta tecnología que los llevará a seguir pistas falsas – mientras las verdaderas amenazas pasan desapercibidas y recursos de por sí limitados son arrebatados al trabajo práctico básico, a la antigua, el único camino que ha frustrado verdaderas conspiraciones terroristas.

(Michael German and Jay Staley, "Whats Wrong with Fusion Centers," American Civil Liberties, diciembre de 2007)

¡Pero tal vez se trata precisamente de "chatarra informática de alta tecnología"!

Después de todo Boeing Company y sus amigos en SRI International (que se describe como "instituto independiente de investigación sin fines de lucro") fueron criticados recientemente por el Subcomité de Ciencia y Tecnología de la Cámara de Representantes por "irregularidades" en el programa Railhead del gobierno, una serie de "actualizaciones" de software del Terrorist Identities Datamart Environment (TIDE) Base de Datos para la Identidad de los Terroristas, "una vasta base de datos que nutre la lista de vigilancia de terroristas," informó Associated Press.

Railhead fue recomendada especialmente como "arreglo" para un sistema creado por Lockheed Martin después de los ataques terroristas del 11-S. Según los investigadores del Congreso, el sistema suministra datos a todas las listas federales de vigilancia de terroristas, incluyendo la lista de "no-vuelo" mantenida por la Administración de Seguridad del Transporte del Departamento de Seguridad Interior y el Centro de Cribado de Terroristas del FBI, un centro nacional coordinador de informaciones para centros de fusión federales, estatales y locales.

Según el comité de la Cámara el sistema tiene un atraso de varios meses, ha excedido su presupuesto en millones y "sería realmente menos capaz que el sistema de rastreo de terroristas del gobierno de EE.UU. que debía reemplazar." La semana pasada The Wall Street Journal informó que:

Cuando fue probado, el nuevo sistema no encontró correspondencias para nombres de sospechosos de terrorismo que habían sido deletreados de un modo ligeramente diferente del nombre registrado en el sistema, un desafío común al traducir nombres del árabe al inglés. Tampoco pudo realizar búsquedas básicas de múltiples palabras relacionadas con conjunciones como "y" y "o". (Siobhan Gorman, "Flaws Found in Watch List for

Terrorists, The Wall Street Journal, 22 de agosto de 2008.)

Dejando de lado las presuposiciones racistas del Journal, a saber, que árabe = terrorista (algo que no carece de importancia cuando se trata con yahoos nativistas aquí en la "patria" o en otros sitios), como dijo el representante Brad Miller (demócrata de Carolina del Norte) en una declaración: "El programa parece estar al borde del colapso después de un gasto que se estima en 500.000 millones de dólares en dineros públicos." Según el comité:

El programa Railhead ha estado sufriendo una implosión técnica interior desde hace más de un año. Pero declaraciones públicas y testimonios públicos jurados ante el Congreso de altos responsables dentro del NCTC Centro Nacional Contraterrorista y la Oficina del Director de Inteligencia Nacional (ODNI) nunca revelaron los crecientes problemas técnicos, la mala administración de contratistas o la descuidada supervisión gubernamental que parecen haber sido endémicas durante todo el programa y que han llevado al colosal fracaso de Railhead. Sorprendentemente, el Director de NCTC y el Director de Inteligencia Nacional han apuntado ambos específicamente a TIDE y NCTC Online como distintivos de los logros del uso compartido de información por el gobierno. ("Technical Flaws Hinder Terrorist Watch List; Congress Calls for Investigation," Committee on Science and Technology, Comunicado de Prensa, 21 de agosto de 2008)

"En un cierto sentido técnico, el NCTC y el ODNI podrán tener razón al recomendar especialmente a la TIDE y a NCTC Online como "distintivos de los logros del uso compartido de información por el gobierno," ¡si con "logros del uso compartido" quieren decir la entrega a contratistas emprendedores de cantidades ilimitadas de billetes que el contribuyente ha ganado con su trabajo!

Gorman informa que en "las últimas semanas, el gobierno ha despedido a la mayoría de los 862 contratistas privados de docenas de compañías que trabajaban en el proyecto Railhead, y sólo queda un personal mínimo." ¿Y la reacción de Boeing y SRI? Según el Journal: "llamados a responsables de Boeing y SRI no fueron devueltos de inmediato."

¡Apuesto a que así fue! Especialmente ya que el comité dijo que "gente informada de Railhead" afirma que el gobierno pagó a Boeing algo como 200 millones de dólares para acondicionar la oficina en Herndon, Virginia de la compañía con mejoras de seguridad para que el ultrasecreto trabajo del software pudiera ser realizado allí. El gobierno luego alquiló el mismo espacio de la oficina a Boeing. ¡No está mal si se trata de encontrar la conocida "zona preferida" de las corporaciones!

Nada de esto, por supuesto, puede sorprender a alguien, menos que a nadie a los miembros del Congreso, adictos a los dólares del lobby de la defensa quienes, como el capitán Renault en Casablanca se sienten "espantados, espantados" al ver que sus "socios" corporativos no han cumplido – una vez más.

Según la lista de Washington Technology de los "máximos 100 contratistas de primera clase del gobierno en 2008" Boeing se registró en el Nº 2 con 9.706.621.413 dólares en entregas de dineros públicos. Siemens, tampoco perezosos, se ubicaron en el Nº 79 con unos 186.292.146 dólares en contratos gubernamentales de primera en una serie de agencias de

defensa y civiles. Con el fin inminente de Railhead, ¿tal vez el gigante electrónico alemán tenga un futuro en el mercado de la “seguridad interior” de EE.UU. con su Plataforma de Inteligencia?

Sin embargo, tal vez no sea así. El experto en seguridad informática Bruce Schneier dijo a New Scientist: “‘actualmente no existen buenos modelos para reconocer a terroristas,’ y cuestiona si Siemens lo ha solucionado.” Pero como lo que le interesa al gobierno es hacer negocios, tal vez lo hagan a pesar de todo.

Mientras tanto, el consorcio PRISE Descripción de la actividad: configuración de realce de la privacidad en la investigación y la tecnología de la seguridad – un enfoque participativo para desarrollar principios aceptables y aceptados para las Industrias y Políticas de Seguridad Europea, N. del T. de expertos en tecnología y derechos humanos financiado por la Unión Europea, pidió “una moratoria en el desarrollo de tecnologías de fusión, refiriéndose explícitamente a la Plataforma de Inteligencia de Siemens,” informó Margottini.

Según New Scientist, analistas de PRISE dijeron a la UE: “La eficiencia y la fiabilidad de semejantes instrumentos son todavía desconocidas. Más vigilancia no conduce necesariamente a un mayor nivel de seguridad de la sociedad. Por ello debe haber un examen exhaustivo de si las masivas restricciones de los derechos humanos resultantes son proporcionadas y justificadas.”

Pero aquí en EE.UU., la preocupación por cosas triviales como las “masivas restricciones de los derechos humanos resultantes,” está indudablemente fuera de discusión, a diferencia de ataques estatales contra los “extraños” derechos del ciudadano promedio, igual como la recusación de un régimen tachonado de criminales de guerra.

Mientras los demócratas celebran esta semana la coronación de Barack Obama en Denver y los republicanos se preparan a hacer lo mismo para John McCain en las “Ciudades Gemelas” Minneapolis y Saint Paul, tranquilizaos: los gobiernos podrán cambiar, pero el fraude corporativo es eterno.

Tom Burghardt es investigador y activista basado en el área de la Bahía de San Francisco. Aparte de publicar en Covert Action Quarterly, Love & Rage y Antifa Forum, es editor de Police State America: U.S. Military "Civil Disturbance" Planning, distribuido por AK Press.

http://www.globalresearch.ca/index.php?context=va&aid=9983

Traducido del inglés para Rebelión por Germán Leyens