PRIVACY INTERNATIONAL

Demanda y oferta: la industria de la vigilancia al descubierto

INFORME ESPECIAL

Demanda y oferta: la industria de la vigilancia al descubierto

Julio 2015

PRIVACY INTERNATIONAL

www.privacyinternational.org

Bogotá desde el cerro de Monserrate.
Crédito: Privacy International (2014).

Índice

Siglas y términos clave

3G	Tercera generación de tecnología de telefonía móvil
4G	Cuarta generación de tecnología de telefonía móvil
ASFADDES	Asociación de Familiares de Detenidos Desaparecidos
CALEA	Communications Assistance for Law Enforcement Act (Ley de Asistencia de Comunicaciones para el Cumplimiento de la Ley) de Estados Unidos
CCAJAR	Corporación Colectivo de Abogados "José Alvear Restrepo"
CIA	Central Intelligence Agency (Organismo Central de Información) de Estados Unidos
DANE	Departamento Administrativo Nacional de Estadística
DAS	Departamento Administrativo de Seguridad
DEA	Drugs Enforcement Agency (Administración para el Control de Drogas) de Estados Unidos
DIJIN	Dirección de Investigación Criminal e INTERPOL
DIPOL	Dirección de Inteligencia Policial
E1	Enlace de telecomunicaciones concebido para transmitir comunicaciones de voz y datos
ELN	Ejército de Liberación Nacional
Esperanza	Plataforma de interceptación gestionada por la Fiscalía
ETSI	European Telecommunications Standards Institute (Instituto Europeo de Normas de Telecomunicaciones)
FARC	Fuerzas Armadas Revolucionarias de Colombia
Fiscalía	Fiscalía General de la Nación
GAULA	Grupos de Acción Unificada por la Libertad Personal
GPS	(Global Positioning System) sistema mundial de localización
GSM	(Global System for Mobile Communications) sistema global de comunicaciones móviles
IMEI	(International Mobile Station Equipment Identity) identidad internacional del equipo móvil
IMSI	(International Mobile Subscriber Identity) identidad internacional del abonado móvil
IP	Protocolo de Internet
ISP	(Internet service provider) proveedor de servicios de Internet
MINTIC	Ministerio de Tecnologías de Información y Comunicaciones
MSC	(Mobile switching centre) centro de conmutación de servicios móviles
OEM	(Original equipment manufacturer) fabricante de equipo original
PGP	Pretty Good Privacy, programa de criptografía de datos
PUMA	Plataforma Única de Monitoreo y Análisis, sistema de vigilancia de las comunicaciones gestionado por la DIJIN
RCS	Remote Control System ("Sistema de Control Remoto"), solución de vigilancia de Hacking Team
SIGD	Sistema Integral de Grabación Digital, sistema de vigilancia de las comunicaciones gestionado por la DIPOL
TAP	(Traffic access point) punto de acceso de tráfico
TMSI	(Temporal Mobile Subscriber Identity) identidad temporal del abonado móvil
TSP	(Telecommunications service provider) proveedor de servicios de telecomunicaciones

Resumen ejecutivo

La industria global de la vigilancia se compone de un grupo creciente de empresas, grandes y pequeñas, que venden tecnologías de vigilancia fundamentalmente a organismos de inteligencia y encargados de hacer cumplir la ley de todo el mundo. En los últimos años ha sido objeto de un mayor escrutinio y crítica por las consecuencias de sus actividades en los derechos humanos y su relación con regímenes represivos, a los que suministra instrumentos de opresión. También en los últimos años, los medios de comunicación han comenzado a informar del uso y abuso que hacen los gobiernos de las tecnologías de vigilancia en contra de activistas, periodistas, disidentes y simples ciudadanos. Pero queda mucho más por saber de la industria de la vigilancia.

La industria de la vigilancia comercial es relativamente nueva. Históricamente, el sector privado ha desempeñado un papel limitado en el suministro de las capacidades de vigilancia que utilizan los organismos estatales de inteligencia y encargados de hacer cumplir la ley. Especialmente en la esfera de la recopilación de información de inteligencia, los Estados han tenido por lo general el monopolio del desarrollo y la utilización de las tecnologías de vigilancia, pues la vigilancia era una actividad intensiva en términos de tiempo y recursos, que exigía un considerable compromiso económico.

El panorama ha cambiado considerablemente en los últimos decenios. Las nuevas tecnologías han puesto la recopilación y retención de cantidades inmensas de datos al alcance presupuestario de cada vez más gobiernos. A mismo tiempo ha surgido la industria comercial, que satisface el interés de los Estados por capacidades de vigilancia cada vez más expansivas. Se calcula que la industria de la vigilancia se valoraba en alrededor de 5.000 millones de dólares en 2011, y crece un 20 por ciento al año.[1] En el material de comercialización de las empresas predomina el discurso de que forman parte de una industria legítima y responsable, cuya finalidad primaria es proteger la seguridad de las personas suministrando tecnologías de vigilancia a los agentes gubernamentales. Estas tecnologías tienen por objeto ofrecer protección frente a la amenaza de aumento de la criminalidad que se cierne como consecuencia de la moderna infraestructura de las comunicaciones.

Sin embargo, las tecnologías de vigilancia pueden servir también a los gobiernos para hostigar a sus detractores, reprimir la disidencia, intimidar a la población, disuadir de ejercer la libertad de expresión y destruir la posibilidad de tener vida privada. Estas tecnologías pueden también utilizarse para someter a poblaciones enteras a monitoreo indiscriminado. En resumen, pueden llegar a ser parte de un aparato estatal de opresión más amplio.

1 “Spies Fail to Escape Spyware in $5 Billion Bazaar for Cyber Arms”, Bloomberg News, 22 de diciembre de 2011, http://www.bloomberg.com/news/2011-12-22/spies-fail-to-escape-spyware-in-5-billion-bazaar-for-cyber-arms.html

Las empresas que venden tecnologías de vigilancia hacen posible y facilitan a menudo la vigilancia estatal violando las normas de derechos humanos; sin embargo, las consecuencias legales y éticas de sus acciones y las tecnologías que venden no han sido nunca objeto de escrutinio en grado suficiente. La serie Demanda y oferta: la industria de la vigilancia al descubierto tiene por objeto demostrar la función del sector privado en el suministro de herramientas de vigilancia a los organismos gubernamentales. Está centrada en el papel de la industria en el diseño, comercialización e instalación de sistemas invasivos de vigilancia; la falta de transparencia en torno a las funciones y los flujos de productos, y la ausencia de procesos de diligencia debida y mecanismos de rendición de cuentas adecuados en materia de derechos humanos.

Este informe forma parte de esa serie y versa sobre Colombia, donde el gobierno lleva más de 50 años combatiendo la insurgencia armada. Varios organismos encargados de hacer cumplir la ley, desde el Departamento Administrativo de Seguridad (DAS) hasta la Dirección de Inteligencia Policial (DIPOL), se han visto implicados en actividades ilegales de vigilancia selectiva de periodistas, activistas y agentes gubernamentales. También el Ejército ha establecido salas de interceptación para espiar las negociaciones de paz e influir en los procesos electorales. En el reciente informe de Privacy International Estado en la sombra: vigilancia y orden público en Colombia se detallan los tipos de tecnologías de vigilancia que utilizan los organismos colombianos de inteligencia y encargados de hacer cumplir la ley. El informe pone al descubierto los intentos del Estado colombiano, en concreto de la Policía, de crear un sistema en la sombra de vigilancia masiva sin autoridad legal clara, salvaguardias contra el uso indebido ni posibilidades de escrutinio público.

A lo largo del último decenio, el gobierno colombiano ha acudido fundamentalmente a empresas privadas con presencia local, así como a empresas de Reino Unido, Estados Unidos e Israel, para abastecerse de equipos de vigilancia. Estas empresas han suministrado tecnologías que posibilitan tanto la interceptación de redes (el monitoreo de los datos y el contenido de las comunicaciones por las redes de los proveedores de servicios) como la interceptación táctica (el monitoreo de los datos y el contenido de las comunicaciones de manera inalámbrica o por dispositivos específicos).

Comenzamos describiendo el Estado de vigilancia de Colombia y los organismos de inteligencia y encargados de hacer cumplir la ley implicados en él. A continuación ofrecemos una perspectiva general del mercado de tecnologías de vigilancia y describimos los tipos de tecnologías que se venden a Colombia y las empresas que las venden. Para concluir, examinamos las responsabilidades legales y éticas de las empresas que equipan al Estado colombiano.

Recomendaciones

A los gobiernos extranjeros y las autoridades encargadas del control de las exportaciones:

- Aprobar legislación que condicione al cumplimento de estrictas disposiciones sobre derechos humanos la asistencia económica y técnica y la transferencia de equipos a organismos de inteligencia, militares o encargados de hacer cumplir la ley de países extranjeros, así como el intercambio de inteligencia con ellos. Tales disposiciones deben prohibir expresamente todo apoyo a personas u organismos de cuya participación en violaciones de derechos humanos haya pruebas o sospechas fundadas.
- Realizar una auditoria exhaustiva de la asistencia prestada en materia de seguridad a los organismos colombianos de inteligencia, militares o encargados de hacer cumplir la ley desde 2000, para determinar si tal asistencia ha dado lugar a violaciones de derechos humanos.
- Revelar públicamente todas las formas de asistencia prestada a Colombia en materia de seguridad, incluidos los datos relativos a la ayuda económica o técnica y la transferencia de equipos a los organismos de inteligencia, militares o encargados de hacer cumplir la ley, así como al intercambio de información de inteligencia con ellos.
- Adoptar estrictos mecanismos de monitoreo del uso final para la asistencia en materia de seguridad a países extranjeros, a través, entre otros medios, de los canales diplomáticos y la participación de la sociedad civil y las instituciones multilaterales.
- Revelar públicamente tales mecanismos de monitoreo del uso final y publicar anualmente los resultados de ese monitoreo de la asistencia en materia de seguridad.
- Adoptar mecanismos legales internos por los que los miembros del Parlamento y la ciudadanía impugnen la prestación de asistencia en materia de seguridad a un país extranjero si tal asistencia ha contribuido o puede contribuir a la comisión de violaciones de derechos humanos.
- No aprobar la exportación de tecnologías de vigilancia reguladas si hay riesgo de que se utilicen para facilitar la represión interna o menoscabar los derechos humanos o si no existe un marco legal claro que regule los usos de los productos exportados.
- Comprometerse a implementar acuerdos sobre medidas de control de las exportaciones relativas a las tecnologías de vigilancia electrónica. Aunque se han tomado ya algunas medidas a raíz del Arreglo de Wassenaar, ello no es óbice para que los gobiernos nacionales y las instituciones regionales, como la Unión Europea, apliquen regulaciones unilaterales.
- Identificar los productos que puedan estar sujetos a permiso de exportación sin perjudicar la investigación en materia de seguridad ni afectar negativamente al desarrollo del sector de las tecnologías de la información y la comunicación. Hay una posible solución que incluiría no sólo la

incorporación del producto a una lista de control del régimen de control de las exportaciones nacional o multilateral, sino también estipulaciones sobre el uso final y el usuario final.

- Garantizar que en las disposiciones sobre el control de las exportaciones se incluyen estrictos criterios de derechos humanos relativos específicamente a las tecnologías de vigilancia. Los criterios de derechos humanos deben tener en cuenta el marco legal del Estado receptor, sus mecanismos de supervisión y su respeto de las normas internacionales de derechos humanos, así como el historial del usuario final con respecto al uso de vigilancia electrónica.
- Trabajar dentro de los regímenes de control de las exportaciones y con instituciones multilaterales y otros Estados para identificar y mitigar las dificultades de aplicar y hacer cumplir los reglamentos de control de las exportaciones sobre las tecnologías de vigilancia, en particular con respecto a las dificultades en materia de intermediación, reexportación, incorporación y desvío.

A las empresas extranjeras y nacionales que venden equipo de vigilancia de las comunicaciones:

- Ejercer la diligencia debida para llevar a cabo investigaciones sobre todo posible usuario final beneficiario antes de acceder a una posible transacción.
- No vender ni suministrar un producto de vigilancia si el usuario final beneficiario del producto no puede ser identificado claramente o presenta un historial documentado de abusos contra los derechos humanos que haya probabilidades de que el producto posibilite.
- No vender ni suministrar un producto a un cliente si no hay un marco legal claro o un mecanismo de supervisión que regulen su uso dentro del país de destino.
- Estipular garantías claras de uso final en los acuerdos contractuales con los clientes, que contengan estrictas salvaguardias de los derechos humanos y protejan contra el uso arbitrario e ilegal.
- Llevar a cabo una revisión periódica y negarse a realizar actividades de mantenimiento, capacitación o actualización si el uso final no cumple estas obligaciones contractuales.
- Elaborar políticas internas sobre los revendedores y distribuidores e incluir en los acuerdos contractuales disposiciones que garanticen que cumplen la normativa de control de las exportaciones y las disposiciones sobre derechos humanos de la propia política.
- Los fabricantes de equipo original (OEM) deben garantizar que la empresa que incorpore su equipo cumple la normativa de control de las exportaciones y las disposiciones sobre derechos humanos del propio OEM.
- Contraer y publicar firmes compromisos de responsabilidad social corporativa (RSC) que se ajusten a la Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos en relación con los derechos humanos.
- Comenzar a realizar una revisión anual del cumplimiento de los compromisos de RSC y las normas internacionales de derechos humanos y publicar los resultados. Tal revisión debe incluir estrictas medidas de transparencia, que contengan, en la mayor medida posible, una lista de usuarios finales.

El Estado de vigilancia colombiano

La interceptación de comunicaciones privadas es una actividad estatal legítima y una restricción admisible del derecho a la privacidad cuando se efectúa de acuerdo con un marco legal claro y detallado, con un fin legítimo y de manera proporcionada a ese fin. Los Estados pueden crear y utilizar una arquitectura de vigilancia de las comunicaciones de manera compatible con las normas internacionales de derechos humanos siempre que lo hagan en un contexto en el que los poderes de vigilancia estén claramente legislados y supervisados y que quienes los ejercen sean transparentes y rindan cuentas a la sociedad.

Las capacidades de vigilancia de los organismos colombianos de inteligencia y encargados de hacer cumplir la ley han ido en aumento a medida que se han ampliado las operaciones militares contra la mayor guerrilla del país, las Fuerzas Armadas Revolucionarias de Colombia (FARC), y su primo pequeño, el Ejército de Liberación Nacional (ELN). [2] El conflicto armado colombiano es el más largo en su género del hemisferio occidental y lleva más de 50 años involucrando a diversos agentes.

El otro agente principal, los grupos paramilitares, que actuaban a veces en colaboración con partes del Estado, se desmovilizó oficialmente a mediados de la década de 2000. También se desmovilizaron varias guerrillas de izquierdas en diversas etapas del conflicto. El conflicto se ha cobrado la vida de casi 220.000 personas,[3] en su mayoría civiles. En el periodo comprendido entre 1985 y 2012 se vieron desplazas internamente 5,7 millones de personas[4] y 25.000 fueron víctimas de desaparición forzada.[5]

En los informes sobre desapariciones forzadas y ejecuciones extrajudiciales abundan las denuncias de interceptación ilegal de comunicaciones privadas. En estas interceptaciones ilegales han participado distintos organismos. En un caso famoso de 2002, los Grupos de Acción Unificada por la Libertad Personal (GAULA), que son unidades conjuntas de la policía y el ejército, interceptaron ilegalmente más de 2.000 líneas telefónicas, según la Fiscalía.[6] Entre los afectados figuraba la Asociación

2 El Departamento de Estado de Estados Unidos ha incluido a ambos grupos en su lista de organizaciones terroristas extranjeras. 2015. http://www.state.gov/j/ct/rls/other/des/123085.htm

3 “Report says 220,000 died in Colombia conflict”, Al Yazira, 25 de julio de 2013, http://www.aljazeera.com/news/americas/2013/07/201372511122146399.html

4 “2015 UNHCR country operations profile – Colombia”, UNHCR, 2015, http://www.unhcr.org/pages/49e492ad6.html

5 “NGO’s remember 25,000 forcibly disappeared in Colombia, call on govt to do more”, Colombia Reports, 22 de mayo de 2014, http://colombiareports.co/ngos-organize-commemoration-week-25000-forcibly-disappeared-colombia/

6 “Informe sobre Derechos Humanos: Colombia”, Departamento de Estado de Estados Unidos, 4 de marzo de 2002, http://www.acnur.org/t3/uploads/media/COI_53.pdf

de Familiares de Detenidos Desaparecidos (ASFADDES), al menos dos de cuyos miembros habían desaparecido también ese año. En 2007 se destituyó a 11 generales de la DIPOL tras saberse que el organismo había intervenido las líneas de teléfono de influyentes políticos de la oposición, periodistas, abogados y activistas.[7] En 2014, el semanario colombiano Semana denunció que una unidad del ejército colombiano con el nombre en clave de "Andrómeda" había estado espiando durante más de un año al equipo negociador del gobierno en las conversaciones de paz entabladas con la guerrilla de las FARC.[8]

Pero el más notorio de los escándalos de interceptación lo protagonizó el Departamento Administrativo de Seguridad (DAS). Los grupos especiales de inteligencia estratégica del DAS sometieron a vigilancia selectiva a alrededor de 600[9] figuras públicas, entre las que había parlamentarios, periodistas, activistas de los derechos humanos, abogados y jueces. El caso lo destapó Semana en febrero de 2009.

Profile

El DAS

Fundado en 1953, el Departamento Administrativo de Seguridad fue uno de los servicios de seguridad de Colombia hasta su disolución, en octubre de 2011, a raíz de que se supiera que había intimidado y sometido a escuchas ilegales a magistrados de la Corte Suprema, trabajadores de derechos humanos, periodistas y políticos de la oposición, y había prestado apoyo a grupos paramilitares violentos. Oficialmente, estaba encargado de producir la información de inteligencia requerida por el Estado, como instrumento de gobierno para la toma de decisiones y la formulación de políticas relacionadas con la seguridad interior y exterior del Estado.[10]

7 "El DAS-gate y las 'chuzadas', vuelve y juega", El Espectador, 21 de febrero de 2009, http://www.elespectador.com/impreso/judicial/articuloimpreso120201-el-das-gate-y-chuzadas-vuelve-y-juega

8 "¿Alguien espió a los negociadores de La Habana?" Semana, 3 February 2014, http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

9 "Más de 600 personas habrían sido 'chuzadas' ilegalmente por el DAS, según investigadores", Caracol Radio, 17 April 2009, http://www.caracol.com.co/noticias/judiciales/mas-de-600-personas-habrian-sido-chuzadas-ilegalmente-por-el-das-segun-investigadores/20090417/nota/446294.aspx

10 Decreto 218, 15 de febrero de 2000, https://www.oas.org/dil/Migrants/Colombia/Decreto%20N°%20218%20del%2015-02-2000.pdf

La magnitud de la intimidación a que sometió el DAS a esas personas es enorme. La vigilancia de las comunicaciones era de gran importancia estratégica. Según los archivos recuperados en el curso de una investigación de la Fiscalía, el DAS interceptó llamadas telefónicas, tráfico de correo electrónico y listas de contactos nacionales e internacionales y utilizó esta información para compilar perfiles psicológicos de los afectados y someter a vigilancia física tanto a ellos como a sus familias, incluidos niños.[11] Uno de los objetivos del DAS fue el periodista Hollman Morris. Las amenazas lo obligaron a exiliarse en varias ocasiones. Claudia Duque, abogada y periodista que había trabajado con el Colectivo de Abogados "José Alvear Restrepo" (CAJAR), sobrevivió a intentos de secuestro y recibió amenazas explícitas de violencia por teléfono. Los archivos del DAS sobre Duque contenían numerosos indicios de vigilancia de las comunicaciones y física.[12] La interceptación ilegal era de tal magnitud, que en el juicio del ex director del DAS en 2011 se recusó a siete magistrados de la Corte Suprema de Justicia porque había información según la cual incluso ellos habían sido víctimas.[13] Ante tantos escándalos, el DAS fue disuelto en octubre de 2011. Su personal fue asignado a otra partes, incluida la Fiscalía, que era la encargada de investigar los abusos del DAS. La directora del DAS en 2008, María del Pilar Hurtado, fue declarada culpable de vigilancia ilegal en febrero de 2015.[14] No obstante, el espectro de la interceptación de las comunicaciones y el incumplimiento de la legislación sobre la vigilancia se cierne todavía sobre el Estado colombiano.

11 Un 'manual' para seguir y acosar a personas calificadas como opositores tenía el DAS", El Tiempo, 13 June 2009, http://www.eltiempo.com/archivo/documento/CMS-5436047

12 "Former security operatives charged in journalist's torture in Colombia", IFEX, 18 de marzo de 2013, https://www.ifex.org/colombia/2013/03/18/security_charged/ y "Colombian official convicted of 'psychological torture' of journalist", Comité para la Protección de los Periodistas (CPJ), 22 de diciembre de 2014, https://cpj.org/2014/12/colombian-official-convicted-of-psychological-tort.php

13 "7 judges withdrawn from wiretap trial", Colombia Reports, 12 de agosto de 2011, http://colombiareports.co/former-das-director-convicted-wiretapping-scandal/

14 "'Chuzadas' del DAS: crimen y castigo", Semana, sábado, 28 de febrero de 2015,

Desde finales de la década de 1990, la interceptación legal de las comunicaciones en las redes colombianas se efectúa por medio de Esperanza –sistema de interceptación gestionado por la Fiscalía, y al que tienen acceso la Policía y, anteriormente, el DAS con miras a iniciar procesamientos judiciales caso por caso.

Desde el punto de vista de su funcionamiento, Esperanza es un sistema de interceptación selectiva, que se basa en solicitudes de usuarios humanos, los administradores de la Fiscalía, para "encargar" a los proveedores de servicios de Colombia que envíen los registros de datos y audio de llamadas de telefonía fija y móvil solicitados específicamente. El uso de Esperanza se rige por la Constitución y Código de Procedimiento Penal colombianos, en los que se establecen con todo detalle los poderes delimitados de la Fiscalía para interceptar legalmente comunicaciones privadas.

Perfil

La FISCALIA

La Fiscalía General de la Nación es una entidad de la rama judicial del poder público con plena autonomía administrativa y presupuestal, cuya función está orientada a garantizar una eficaz administración de justicia.[15] Establecida en 1991, se encarga de llevar a cabo investigaciones criminales con miras a iniciar procesamientos judiciales, garantizar la protección de las víctimas y testigos y dirigir y coordinar la funciones de la policía judicial. La Fiscalía es responsable de administrar la plataforma Esperanza y de examinar y aprobar las órdenes de interceptación de otros organismos, entre ellos el DAS y la Policía. La Fiscalía dirige la investigación que se está llevando a cabo sobre las escuchas ilegales realizadas por el DAS a mediados de la década de 2000 haciendo uso indebido, según informes, de los privilegios de acceso a la plataforma Esperanza.

En los últimos años, la capacidad de interceptación de las comunicaciones se ha ampliado para abarcar también la interceptación masiva y automatizada de tráfico telefónico y de correo electrónico en la troncal de la infraestructura de telecomunicaciones de la nación. Esta actividad constituye vigilancia masiva. Se pueden barrer, filtrar, monitorear y analizar las comunicaciones de millones de personas antes de almacenarlas para su posterior examen o borrarlas, aun cuando esas personas no sean sospechosas de nada ilícito. A diferencia de las formas tradicionales de interceptación selectiva, la interceptación automatizada permite interceptar en masa cables completos colocando un sonda directamente en el cable. Los componentes del sistema clasifican, almacenan, reagrupan en paquetes y reúnen de nuevo los datos interceptados, según cómo estén programados.

La Plataforma Única de Monitoreo y Análisis (PUMA) se presentó en 2007como sistema de "monitoreo" administrado y costeado por la Policía y gestionado por la DIJIN. La tecnología con que está creada permite la interceptación masiva, pasiva e indiscriminada de las comunicaciones de la ciudadanía colombiana.

15 ¿Quiénes somos?", Fiscalía, 2015, http://www.fiscalia.gov.co/colombia/la-entidad/quienes-somos/

Perfil

La DIJIN

La Dirección de Investigación Criminal e Interpol es la unidad de policía a cargo de la investigación judicial. Es una de las ocho direcciones de policía de la Dirección General de la Policía Nacional, que depende del Ministerio de Defensa. Su función consiste en apoyar la investigación criminal en las áreas técnicas, científicas y operativas, por iniciativa propia o según orden impartida por la Fiscalía. Los agentes de la DIJIN han aportado competencia forense a las investigaciones de interceptaciones ilegales.

La DIPOL también gestiona un sistema que intercepta volúmenes enormes de señales de comunicaciones, así como datos que no son de comunicaciones, por medio de sondas de red conectadas a una plataforma centro de monitoreo. Este centro de monitoreo recibe, procesa y retiene datos recopilados por diversas fuentes de datos, como monitoreo de Internet, monitoreo de ubicaciones, monitoreo de teléfonos y vídeo y audio vigilancia. Una vez recopilados, estos datos son analizados con potentes programas informáticos que muestran conexiones entre personas. Estableciendo vínculos entre las personas y sus contactos y entre los contactos de esas personas, los analistas pueden elaborar perfiles de ellas y de sus contactos y acceder a sus comunicaciones privadas basándose únicamente en sus patrones de comunicación. Dependiendo de cómo estén programados los componentes de la tecnología, todo este análisis puede tener lugar antes incluso de que un ser humano vea los datos interceptados.

Perfil

La DIPOL

La Dirección de Inteligencia Policial, DIPOL es la unidad de policía responsable de producir información de inteligencia estratégica y operativa relacionada con cuestiones de alteración de orden público, seguridad y defensa. Se encarga de realizar actividades de contrainteligencia nacional.[16] Es una de las ocho direcciones de policía de la Dirección General de la Policía Nacional, que depende del Ministerio de Defensa. La DIPOL se ocupa también de dirigir los planes de desarrollo tecnológico con respecto a las actividades de inteligencia dentro de la Policía. Los agentes de la DIPOL han sido acusados de interceptaciones ilegales contra periodistas. [17]

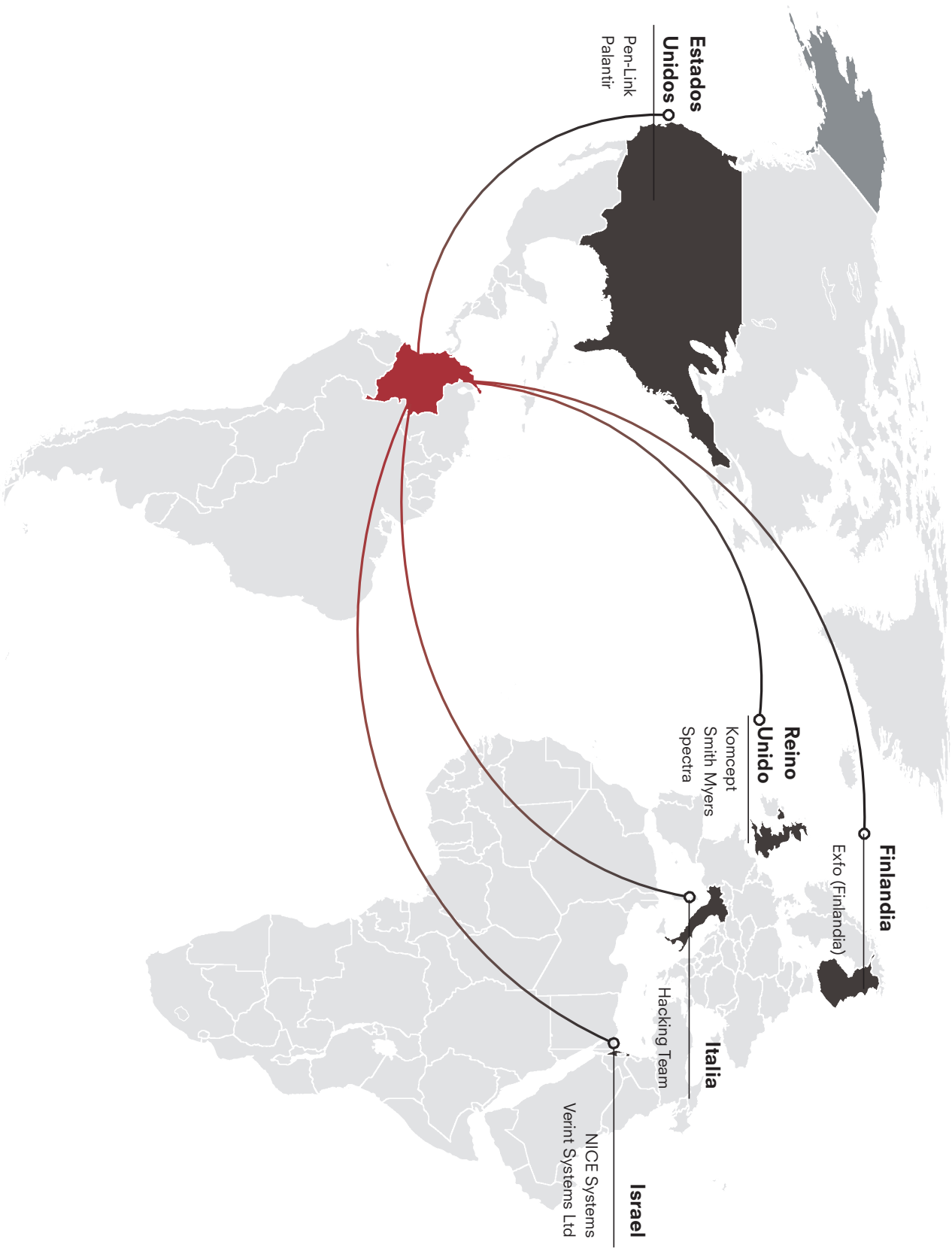
16 "Dirección de Inteligencia Policial", Colombia National Police, 2015, http://oasportal.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones_tipo_Operativas/Direccion_Central_Inteligencia

17 "Senior intelligence chiefs suspended or resign over scandal on tapping of journalists' and politicians' telephones", IFEX, 2 July 2007, http://www.ifex.org/colombia/2007/07/06/senior_intelligence_chiefs_suspended/

En 2012, la DIPOL negoció también la compra de potente tecnología de inteligencia de código abierto que le habría permitido basarse en su plataforma ya existente para analizar y procesar enormes cantidades de datos y comunicaciones, desde interacciones de Facebook hasta datos biométricos, y extraer conclusiones sobre la probabilidad, por pequeña que fuera, de participación de las personas en actividades delictivas pasadas o futuras. Además, la Policía adquirió software de intrusión que posibilitaba la explotación selectiva a distancia –¬en esencia, el hackeo y control– de los dispositivos de la gente. Tal tecnología, proporciona al usuario, en este caso, la Policía, capacidades extraordinarias, como activar a distancia el micrófono y la cámara del teléfono o el ordenador del objetivo y ver u escuchar así todo lo que ocurre cerca del dispositivo.

Los organismos del Estado que adquieren estas capacidades lo hacen no sólo al margen del escrutinio público, sino también sin autorización legal. Ninguno de los organismos antedichos está autorizado a realizar actividades de "interceptación" sin la supervisión de la Fiscalía. La Constitución y el Código de Procedimiento Penal disponen que la interceptación de comunicaciones sólo puede hacerse a través de la Fiscalía, en el marco de una investigación judicial y de manera selectiva. El marco legal colombiano que regula la vigilancia de las comunicaciones adolece de fatales errores técnicos y legales, que se examinan detenidamente en el informe de Privacy International Estado en la sombra: vigilancia y orden público en Colombia.

La venta de vigilancia



Selección de empresas cuyos productos de vigilancia se han vendido a organismos colombianos de inteligencia y encargados de hacer cumplir la ley

El gobierno colombiano ha adquirido una cantidad considerable de material de vigilancia de las comunicaciones. Lo suministran en su mayor parte empresas extranjeras, por medio de socios colombianos.

Los fondos para tecnología de vigilancia se dispararon con el "Plan Colombia", programa conjunto de asistencia militar de Estados Unidos y Colombia, desarrollado a finales de la década de 1990. Las fuerzas militares están especialmente bien financiadas: en 2015, el presupuesto de defensa de Colombia es de 14.170 millones de dólares estadounidenses, lo que convierte el sector en el segundo mejor financiado.[18]

Colombia asiste a varias ferias de tecnología de vigilancia y seguridad, y acoge también algunas. La "Intelligence Support Systems World" (ISS World), conocida también como "Wiretappers' Ball" ("Baile de los escuchas") , es una de las ferias más grandes y está centrada en proveedores norteamericanos y europeos. La policía colombiana asistió a la ISS World en 2012, cuando exhibieron sus productos tres empresas colombianas: Biotekne SAS, Colombia ASOTO Technology Group y la empresa ensambladora del sistema de vigilancia Esperanza, STAR Colombia Inteligencia & Tecnología (STAR).[19] La feria y conferencia anual Cibercolombia, donde se exhiben fundamentalmente productos de vigilancia israelíes está financiada por la embajada de Israel en Bogotá.[20]

Gran parte del material de seguridad de Colombia lo suministran empresas internacionales, en especial estadounidenses. A lo largo del último decenio, los fondos, el material y la capacitación estadounidenses suministrados a las unidades de élite de los servicios de inteligencia colombianos se utilizaron, según informes, para espiar a magistrados de la Corte Suprema, opositores políticos del entonces presidente Álvaro Uribe y grupos de la sociedad civil. Las comunicaciones interceptadas eran esenciales para las operaciones encubiertas colombianas y del Organismo Central de Información (CIA) de Estados Unidos contra las FARC.[21] Aunque la legislación colombiana sobre contratación pública, Ley 80 de 1993, concede prioridad a los artículos de seguridad y defensa nacional producidos en Colombia por fabricantes locales,[22] una salvedad, relativa al trato nacional, del acuerdo bilateral de comercio entre Estados Unidos y Colombia de 2006 permite tratar a las empresas estadounidenses como empresas locales cuando participan en concursos públicos.[23] Israel también es un importante proveedor militar. La empresa israelí-estadounidense Verint Systems suministró infraestructura de interceptación decisiva, utilizada por el DAS, la DIPOL y la DIJIN al menos desde 2005. Verint Systems Ltd., es el socio israelí de Verint Systems Inc, radicada en Estados Unidos.

18 "Crunching the numbers on Colombia's 2015 budget", Colombia Reports, 26 de agosto de 2014, http://colombiareports.co/crunching-numbers-colombias-2015-budget/

19 "Program Schedule for Year 2013", ISS World, 2012, https://www.wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf

20 "Conference Ciber Colombia 2015", Instituto de Cooperación Internacional y Exportación de Israel, 2015, http://www.export.gov.il/heb/Branches/Technologies/DefenceIndustries/Events/events,1418

21 "U.S. aid implicated in abuses of power in Colombia", The Washington Post, 20 de agosto de 2011, http://www.washingtonpost.com/national/national-security/us-aid-implicated-in-abuses-of-power-in-colombia/2011/06/21/gIQABrZpSJ_story.html

22 Decreto 734 de 2012, 13 de abril de 2012, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=46940#0

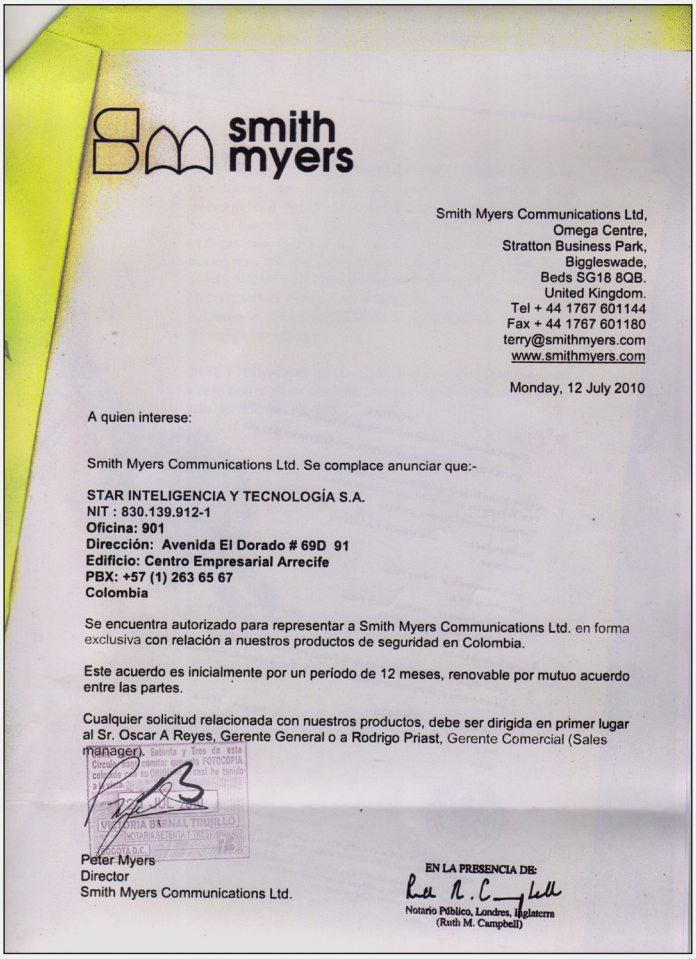
23 "Chapter Nine: Government Procurement", Oficina del Representante de Comercio de los Estados Unidos, 2006, http://www.ustr.gov/sites/default/files/uploads/agreements/fta/colombia/asset_upload_file739_10140.pdf

UN VARIADO SURTIDO

Pequeña selección de productos de interceptación táctica a la venta en Colombia: tarjeta de crédito grabadora de la empresa suiza Nagra; 'Pointer', radiogoniómetro manual de la empresa británica Smith Myers Communications que se utiliza cuando se interceptan llamadas telefónicas con un IMSI catcher, y grabadora de vídeo y audio que imita una silla para bebé, de la empresa británica LMW Electronics.

Los productos de vigilancia adquiridos por los organismos colombianos en el sector privado son en general de dos tipos: productos necesarios para interceptación de redes y productos que facilitan la interceptación táctica. Normalmente, el gobierno colombiano compra las sondas de red y los centros de monitoreo necesarios para los programas de interceptación de redes a grandes vendedores internacionales, por medio de empresas colombianas que tienen acuerdos de exclusividad para distribuir los productos de determinados vendedores internacionales o que los representan legalmente en los contratos directos con los clientes gubernamentales.

Entre tales asociaciones figuran, por ejemplo, las de: Verint Systems y la Compañía Comercial Curacao de Colombia (La Curacao); la empresa estadounidense DreamHammer y su representante en Colombia, Emerging Technologies Corporation;[24]



smith myers

Smith Myers Communications Ltd,
Omega Centre,
Stratton Business Park,
Biggleswade,
Beds SG18 8QB.
United Kingdom.
Tel + 44 1767 601144
Fax + 44 1767 601180
terry@smithmyers.com
www.smithmyers.com

Monday, 12 July 2010

A quien interese:

Smith Myers Communications Ltd. Se complace anunciar que:-

STAR INTELIGENCIA Y TECNOLOGÍA S.A.
NIT : 830.139.912-1
Oficina: 901
Dirección: Avenida El Dorado # 69D 91
Edificio: Centro Empresarial Arrecife
PBX: +57 (1) 263 65 67
Colombia

Se encuentra autorizado para representar a Smith Myers Communications Ltd. en forma exclusiva con relación a nuestros productos de seguridad en Colombia.

Este acuerdo es inicialmente por un período de 12 meses, renovable por mutuo acuerdo entre las partes.

Cualquier solicitud relacionada con nuestros productos, debe ser dirigida en primer lugar al Sr. Oscar A Reyes, Gerente General o a Rodrigo Priast, Gerente Comercial (Sales manager).

Peter Myers
Director
Smith Myers Communications Ltd.

EN LA PRESENCIA DE:
Notario Público, Londres, Inglaterra
(Ruth M. Campbell)

HACIENDO NEGOCIOS

Las empresas extranjeras de vigilancia hacen negocios en Colombia por medio de empresas locales con las que tienen acuerdos de exclusividad, como éste firmado entre Smith Myers Communications y STAR.

24 "DreamHammer Signs Drone Software Distribution Deal to Service Colombian Government Through Partner, Emerging Technologies Corporation", Business Wire, 15 de mayo de 2014, http://www.businesswire.com/news/home/20140515006450/en/DreamHammer-Signs-Drone-Software-Distribution-Deal-Service#.VM9YFId3aT8

la empresa británica Smith Myers Communications y su representante, STAR desde 2010, y la empresa estadounidense Harris y la canadiense Allen-Vanguard con la empresa representante de ambas Eagle Commercial SA.[25] Es frecuente que las empresas locales colombianas tomen prestado material de los proveedores internacionales para hacer demostraciones de productos a los posibles clientes gubernamentales.

Otra forma habitual de presentarse a las licitaciones es que dos o más empresas colombianas que representan a empresas extranjeras formen una unión temporal para poder cumplir mejor los requisitos técnicos de la licitación. Estas uniones suelen disolverse al final del contrato. Otras empresas licitadoras en Colombia, como la alemana Rohde & Schwarz, crean filiales colombianas legalmente independientes.

Con algunas excepciones, las empresas colombianas no producen el material necesario para la interceptación de redes en el país. No obstante, sí se fabrican localmente componentes simples de los sistemas de vigilancia, como consolas de monitoreo por circuito cerrado de televisión (CCTV) y las pantallas y ordenadores en que se analiza la información interceptada. Algunas empresas integran sus propios sistemas de interceptación táctica, como Emerging Technologies Corporation, que está desarrollando tecnología de drones DreamHammer, empresa radicada en California[26], y STAR, que fabrica varios productos de interceptación de redes de marca registrada.[27] La importación de artículos militares y policiales fabricados en el extranjero está exenta de impuestos, y el material de vigilancia lo importan directamente los organismos contratantes, aunque el contratista es responsable legalmente de la integridad de los artículos.[28]

25 "Importador de inteligencia", El Espectador, 27 de mayo de 2011, http://www.elespectador.com/noticias/wikileaks/importador-de-inteligencia-articulo-259259

26 "DreamHammer Signs Drone Software Distribution Deal to Service Colombian Government Through Partner, Emerging Technologies Corporation", Business Wire, 15 de mayo de 2014, http://www.businesswire.com/news/home/20140515006450/en/DreamHammer-Signs-Drone-Software-Distribution-Deal-Service#.VM9YFId3aT8

27 "STAR Inteligencia & Tecnología", STAR Inteligencia & Tecnología, 2015, http://www.STAR-it.co

28 "Adquisición de Sistemas para el Fortalecimiento Tecnológico de la Plataforma Única de Monitoreo y Análisis (PUMA)", Dirección Administrativa y Financiera, Ministerio de Defensa, 26 de noviembre de 2013.

Interceptación de redes

Las tecnologías de interceptación de redes son herramientas en las que es necesaria la instalación física en una red para llevar a cabo la vigilancia de las comunicaciones. Estas herramientas son la versión moderna, más compleja y potente, de las pinzas de cocodrilo que se utilizaban hace años. Hay que distinguir las tecnologías de interceptación de redes de las tecnologías de interceptación táctica, herramientas de vigilancia móvil que no es necesario instalar físicamente en una red, sino que reciben los datos de manera inalámbrica o directamente de los dispositivos.

Normalmente, para la creación de una plataforma de interceptación de redes son necesarios tres tipos de agentes comerciales, que suministran distintas clases de productos y servicios. El primer tipo de agente comercial es el fabricante del equipo que sirve de base a una red; son ejemplos de este tipo Nokia, Huawei y Alcatel-Lucent. Entre el material que suministran estas empresas figuran switches e intercambiadores que se utilizan para conectar tráfico entre líneas, así como otro hardware y servicios que garantizan que la infraestructura de telecomunicaciones en su conjunto pueda mantener diferentes redes y servicios.

El segundo tipo de agente comercial es el proveedor de servicios de telecomunicaciones (TSP), que gestiona la red y cobra a los abonados por los servicios. Los TSP son responsables de garantizar que sus actividades cumplen la legislación nacional del país donde operan. Tal responsabilidad comporta normalmente la obligación legal de que el TSP facilite el acceso de los organismos de seguridad y encargados de hacer cumplir la ley a sus redes y a los datos de sus abonados. En Colombia, los proveedores de servicios acceden a las solicitudes de interceptación de los organismos encargados de hacer cumplir la ley previa autorización de la Fiscalía, según el Decreto 1704 del Ministerio de Tecnologías de Información y Comunicaciones (MINTIC).[29]
El artículo 44 de la Ley de Inteligencia de 2013 también dispone que los proveedores de telecomunicaciones deben acceder a las solicitudes de acceso a datos y de otras formas de asistencia técnica de los organismos de inteligencia y contrainteligencia.

El tercer tipo de agente comercial es la empresa de tecnología de vigilancia que comercializa directamente productos y servicios con fines de cumplimiento de la ley. Estas empresas suministran "soluciones" dirigidas a posibilitar a los organismos de encargados de hacer cumplir la ley interceptar, analizar o difundir datos de redes. Las empresas de vigilancia venden estas soluciones directamente a los gobiernos o a organismos concretos o, si no, a los TPS a fin de que cumplan con la obligación legal vigente en muchos países de que los TSP adapten sus redes de manera que faciliten la interceptación legal. Como consecuencia de ello, algunos TSP negocian por su propia cuenta con las empresas de vigilancia e incorporan soluciones de vigilancia electrónica a sus redes.

29 Decreto número 1704 de 15 de agosto de 2012, Ministerio de Tecnologías de Información y Comunicaciones, 15 de agosto de 2012, http://www.mintic.gov.co/portal/604/articles-3559_documento.pdf

En todo el mundo, incluida Colombia, los gobiernos exigen que los TSP hagan compatibles sus redes aplicando y haciendo cumplir normas de "interceptación legal". La Ley de Asistencia de Comunicaciones para el Cumplimiento de la Ley (Communications Assistance for Law Enforcement Act, CALEA) en Estados Unidos y la normas del Instituto Europeo de Normas de Telecomunicaciones (European Telecommunications Standards Institute, ETSI) en Europa son dos ejemplos de marco legal concebido para garantizar que todos los fabricantes de equipos para redes de telecomunicaciones y todos los TSO diseñan infraestructura de telecomunicaciones accesible para los Estados. Normalmente, en las convocatorias de licitación para equipos de interceptación de comunicaciones se exige que la tecnología cumpla la CALEA.[30]

Colombia (2012)

Población (2013):	48.321.405 (Banco Mundial)
Abonados de telefonía fija (2013):	7.141.461[31] (MINTIC)
Abonados de telefonía móvil (2012):	49.066.359 (MINTIC)[32]
Subscritores a Internet fijo (2012):	4.047.032 (MINTIC)
de los cuales, con banda ancha (2012):	3.918.266 (MINTIC)
Porcentaje de personas que utilizan Internet (2013):	51,7% (DANE)[33]

30 "Asunto; Respuesta observaciones, Adquisición construcción y desarrollo tecnológico – Equipo de Monitoreo de Telefonía Móvil Celular Nueva Tecnología – Sistema Integral de Grabación Digital – con Destino a la Policía Nacional", Fondo Rotatorio de la Policía, Ministerio de Defensa Nacional, 25 de febrero de 2005.

31 "Fixed Telephone Subscriptions (Excel)",Unión Internacional de Telecomunicaciones, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

32 "Boletín trimestral de las TIC Cifras cuarto trimestre de 2012", MINTIC, marzo de 2013, http://www.mintic.gov.co/images/documentos/cifras_del_sector/boletin_4t_banda_ancha_vive_digital_2012.pdf

33 "Percentage of Individuals using the Internet", Unión Internacional de Telecomunicaciones, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Proveedores de servicios de telefonía móvil (2014) [34]

Total de abonados	51.594.619

Proveedor	**Porcentaje del total de abonados**
Comcel	56,61%
Movistar	23,97%
Tigo	15,42%
Uff Móvil	0,79%
Une EPM	0,68%
Avantel	0,39%
ETB	0,09%
Virgin Mobile	1,66%
Éxito	0,38%

34 "Telefonía móvil: Participación en total de abonados por proveedor", MINTIC, 2014, http://estrategiaticolombia.co/estadisticas/stats.php?&pres=content&jer=1&cod=&id=86#TTC

Las empresas: interceptación de redes

En este apartado se examinan las tecnologías de interceptación de redes presentes en Colombia en los últimos cinco años y las empresas nacionales y extranjeras que las suministran.[35]

STAR construyó la plataforma de interceptación móvil y fija de ámbito nacional Esperanza utilizando fundamentalmente su propia tecnología y productos de la empresa estadounidense Pen-Link y de la británica Komcept Solutions.

Verint Systems Ltd. construyó el Sistema Integral de Grabación Digital de la Policía con sus propias soluciones de interceptación Vantage y Reliant, suministradas y mantenidas por La Curacao. Verint Systems montó también el sistema de interceptación PUMA de la Policía. Otra empresa israelí, NICE Systems, consiguió, en unión con la colombiana Eagle Commercial, varios contratos posteriores para la ampliación en gran escala de la capacidad de interceptación de PUMA.

Otras empresas descritas en este informe, que venden productos de interceptación de redes en Colombia, son la neerlandesa Digivox y la estadounidense NetworkCritical.

STAR Inteligencia & Tecnología y la plataforma Esperanza

STAR se registró como empresa en mayo de 2004 y, durante los dos años siguientes, trabajó exclusivamente en la creación de la plataforma Esperanza.

STAR creó Esperanza integrando componentes de proveedores fundamentalmente británicos y estadounidenses en sus propios equipos para montar una plataforma a medida. En la actualidad, STAR suministra hardware y software de interceptación, plataformas de análisis de grandes cantidades de datos (big data) y centros de mando y control, entre otras soluciones de seguridad, y es el único distribuidor autorizado de los productos de varias empresas internacionales. Asimismo, es una de las pocas empresas de propiedad colombiana que suministra su propio material de interceptación de redes de marca registrada.

Komcept Solutions suministró su plataforma Elucidate a STAR en el marco de Esperanza. Komcept Solutions vende equipos de interceptación legal a clientes gubernamentales desde su sede rural de Northamptonshire desde 2001.[36] Entre

35 Este informe no contiene una lista exhaustiva de las empresas que hay en Colombia o venden tecnología de vigilancia al país, sino un análisis de algunos de los proveedores de tecnología de vigilancia más importantes y de los que son parte integrante de los proyectos de interceptación de redes del Estado colombiano. Las empresas descritas en el informe suelen incluir en su catálogo tecnología tanto de interceptación de redes como de interceptación off-the-air (por el aire).

36 “Komcept Solutions Ltd.”, registro mercantil británico, 2015,

los productos del catálogo de Komcept Solutions figura también un dispositivo portátil de grabación de audio con aspecto de maletín, que contiene 144 micrófonos digitales, y un procesador digital de señales que puede grabar a una distancia de hasta 30 metros y transmitir los datos por Bluetooth a un analista ubicado lejos de allí.[37] Una empresa registrada en Panamá y propiedad de los ejecutivos de STAR, Expert Design Solutions, se encarga del mantenimiento de los equipos de Komcept Solutions en Panamá, Reino Unido y Estados Unidos.

STAR COLOMBIA
Inteligencia & Tecnología

SALA SECCIONAL
Conectada con
PLATAFORMA CONTROL TELEMÁTICO

ITEM	DESCRIPCIÓN	CANTIDAD	VALOR UNIDAD	VALOR TOTAL
1	Sistema de Grabación ELUCIDATE-KOMCEPT: - Un (1) Sistema Elucidate: - 1 TB de almacenamiento. - Señal recibida desde sala Plataforma Control Telemático. - Equipos de interconexión. - Un (01) PRI o un (01) E1.	1	$ 330'000.000	$ 330'000.000
	- Capacitación técnica y administrativa de los equipos que componen el sistema.		**Incluida en el costo**	

Sub TOTAL	$ 330'000.000
IVA (16%)	$ 52'800.000
TOTAL	**$ 382'800.000**

NOTA: La Fiscalía General de la Nación debe suministrar un canal de comunicación entre la Plataforma de Control Telemático ubicada en el Búnker de la Fiscalía General de la Nación en Bogotá y la sala de monitoreo de la seccional a instalar, con el fin de realizar la transmisión de los datos y el audio enviados.

Validez de la Oferta: Un (01) mes.
Tiempo de Entrega: Tres (03) meses.
Precios: Los valores están dados en pesos colombianos.
Garantía: Los sistemas ofrecidos cuentan con una garantía de un (1) año contra defectos de fabricación. Se realizarán dos (02) visitas de mantenimiento preventivo. Se asignará un ingeniero como punto de contacto para requerimientos de soporte del sistema.

NOTA: Komcept (casa matriz) ha autorizado un descuento especial para la Fiscalía General de la Nación por un 50% de costo del equipo cotizado antes de impuestos. A continuación presentamos de nuevo la cotización con el descuento correspondiente.

Av El Dorado, # 68 C 61 Of 327 - 3 PBX (+57 1) 427 5077 FAX (+57 1) 427 5076 EMAIL star@star-colombia.cor
www.star-colombia.com

CON DESCUENTO

Komcept Solutions hizo descuentos especiales a la Fiscalía para que utilizara su plataforma 'Elucidate'

37 "DSEi 2009n Exhibition Show Preview", Defence Business, 2009, http://issuu.com/karlosullivan/docs/dbjuly

La empresa estadounidense de tecnología Pen-Link suministró la interfaz de Esperanza que los agentes colombianos utilizarían para gestionar y analizar el contenido y los datos de los teléfonos interceptados. En 2010, la mitad del negocio de Pen-Link era con Latinoamérica[38], y la empresa celebra conferencias en Bogotá para ofrecer formación sobre el uso de sus productos a funcionarios encargados de hacer cumplir ley de toda la región que asisten a ellas.[39] Pen-Link vende también una plataforma para servidores llamada "Lincoln", en la que se alojan los datos interceptados. Lincoln puede "recibir información de interceptaciones en tiempo real transmitida por los operadores para cualquiera de las interceptaciones autorizadas legalmente del organismo". El proceso de recopilación en sí está controlado por el software cliente Pen-Link 8.[40] Pen-Link es uno de los proveedores preferidos de la Administración para el Control de Drogas (Drugs Enforcement Agency, DEA) de Estados Unidos, habiendo participado en 170 contrataciones del organismo desde 1995, la mayoría en los últimos cuatro años.[41] Pen-Link suministró también a la embajada de Estados Unidos en Bogotá "software de enlace específico", de cuyo mantenimiento periódico se ocupó durante años.[42]

A lo largo del periodo de ejecución del contrato de Esperanza, STAR mantuvo vínculos muy estrechos con la Fiscalía. En 2009, el ingeniero de STAR a cargo del sistema Esperanza, que se ocupaba de administrarlo y de corregir los fallos, así como de la planificación, desarrollo y gestión, dependía directamente del director de sistema Esperanza de la Fiscalía, Vladimir Flórez Beltrán. STAR invitó a Beltrán a almuerzos en 2008 y 2009. En 2011 STAR corrió también con los gastos de billetes, hotel y demás costes de viaje de otro funcionario de la Fiscalía que tuvo que viajar a Reino Unido para verifica dos vehículos de vigilancia para los que tenía un contrato de compra con la empresa británica LMW Electronics en 2011. Asimismo, STAR tuvo una cuenta conjunta con la Fiscalía en 2010, según la correspondencia que se muestra en los anexos de este informe.

Su proximidad a la Fiscalía y su papel central en la instalación del sistema de interceptación más conocido de Colombia aportaron a STAR muy buenas relaciones en los círculos de contratación de defensa. STAR tenía contacto con las principales ramas de los servicios militares y policiales y con las embajadas británica, estadounidense y mexicana. El director de STAR, Oscar Reyes, y sus directores comercial y de proyectos hicieron viajes de negocios a Londres, Los Ángeles y Nueva York para suscribir y finalizar contratos con proveedores. Otros técnicos de la

38 "Mike Murman shares field notes from growing businesses", Nebraska Entrepreneurship, 15 de diciembre de 2010, http://www.nebraskaentrepreneurship.com/news/mike-murman-shares-field-notes-from-growing-businesses/

39 "2012 Pen-Link Latin American Technical Training", Pen-Link, 15 de marzo de 2012 http://www.penlink.com/News/tabid/96/Default.aspx

40 "Lincoln Collection Systems", Pen-Link, 2015, http://www.penlink.com/Products/tabid/54/Default.aspx

41 "Contract Actions: Vendor Name: Pen-Link, Ltd., Department Full Name: Department of Justice," Administración de Servicios Generales de Estados Unidos, 20 de abril del 2015, https://www.fpds.gov/ezsearch/fpdsportal?s=FPDSNG.COM&q=pen-link+VENDOR_FULL_NAME%3A%22PEN-LINK%2C+LTD.%22+CONTRACTING_AGENCY_NAME%3A%22DRUG+ENFORCEMENT+ADMINISTRATION%22&indexName=awardfull&y=0&templateName=1.4.4&x=0&STARt=0

42 "Contract Actions: Vendor Name: Pen-Link, Ltd., Department Full Name: Department of State," Administración de Servicios Generales de Estados Unidos, 20 de abril de 2015, https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.4.4&s=FPDSNG.COM&q=PEN-LINK+DEPARTMENT_FULL_NAME%3A%22STATE%2C+DEPARTMENT+OF%22+CONTRACTING_OFFICE_NAME%3A%22AMERICAN+EMBASSY+-+BOGOTA+-+GSO%22&x=0&y=0

empresa viajaron mucho por toda Colombia para aplicar los proyectos de vigilancia de STAR contratados. Varios técnicos de STAR se turnaban los fines de semana para ocuparse de los fallos de la salas de interceptación del DAS durante 2009 y 2010.

El modelo de gestión funcionó. Las ventas de STAR se multiplicaron por 10 durante sus primeros años, pese a que tenía sólo 11 empleados en 2009. Ese año tenía aproximadamente 1.200 millones de pesos colombianos (alrededor de 540.000 dólares colombianos) de reservas, y más del 90 por ciento de los ingresos que recibía de empresas cuya tecnología vendía eran de compañías extranjeras, más que colombianas. Un verdadero negocio familiar: el 75 por ciento de las participaciones de STAR son de la familia de Oscar Reyes.

Verint Systems, La Curacao y las plataformas de la Policía

Verint Systems Ltd., socio israelí de Verint Systems Inc., radicada en Estados Unidos, vendió tecnología de vigilancia masiva a la policía colombiana.

A mediados de la década de 2000, la Policía había empezado a pedir una ampliación de sus capacidades de interceptación debido a las deficiencias de Esperanza. En particular, le preocupaban los cupos de interceptación de la plataforma, sus disfunciones técnicas y su falta de capacidad para gestionar el creciente volumen de comunicaciones basadas en el protocolo de Internet (IP). El sistema de interceptación PUMA se presentó en 2007 como sistema de "monitoreo" administrado y costeado por la DIJIN.

PUMA está basado en una tecnología considerablemente más potente e invasiva que la de Esperanza. Utiliza tecnología concebida específicamente para recopilar todos los datos que pasan por los cables para su posterior análisis. En este sentido, es un sistema "pasivo", en el que no es necesario que intervenga un agente de la Fiscalía para recuperar la información del proveedor de servicios. Al contrario, el sistema está enlazado directamente con la infraestructura de red de los proveedores de servicios, normalmente en el centro de conmutación móvil, por medio de una sonda que direcciona directamente todos los datos al centro de monitoreo del organismo encargado de hacer cumplir la ley sin interferir en la transmisión de los datos entre el emisor y el receptor.

Más o menos a la vez que se instalaba PUMA, otra dirección de la Policía construyó una plataforma de interceptación, el Sistema Integral de Grabación Digital (SIGD), con la misma tecnología que PUMA. El SIGD podía monitorear el tráfico masivo de comunicaciones por las troncales E1 y también el tráfico de telefonía móvil 3G. No estaba limitado a la vigilancia selectiva, pues, como se explica en la documentación disponible, podía generar nuevos objetivos.

La rama israelí de Verint Systems suministró la tecnología con que la Policía creó PUMA y el SIGD. Verint Systems Inc., radicada en Estados Unidos, es una empresa fabricante de software y hardware, especializada en soluciones de inteligencia y análisis de datos, mientras que Verint Systems Ltd. tiene productos de vigilancia de las comunicaciones. Verint Systems era parte en su origen de Comverse Technology,

pero en 2013 adquirió la participación de ésta. Comverse Technology fue fundada en Israel por, entre otros, Jacob 'Kobi' Alexander, quien en 2006 estuvo implicado en un grave escándalo de alteración de fechas de acciones.[43] Como se informó durante la década de 2000, Verint Systems participó en el suministro de material para escuchas telefónicas a Verizon durante el escándalo de las escuchas sin orden judicial del Organismo de Seguridad Nacional (NSA) de Estados Unidos.[44]

Con 910 millones de dólares estadounidenses de ingresos en 2014,[45] Verint Systems forma parte del pequeño grupo de líderes mundiales de la tecnología para centros de monitoreo. En su catálogo de material de comunicaciones y ciberinteligencia, vende soluciones de ciberseguridad, tecnología de rastreo móvil, dispositivos de interceptación táctica que sirven para interceptar llamadas de móviles y herramientas analíticas de código abierto. Por ejemplo, su sistema SkyLock se presenta como una herramienta capaz de rastrear la ubicación de un teléfono móvil en cualquier lugar del mundo.[46] Con la vista puesta en los TSP y los organismos de inteligencia y encargados de hacer cumplir la ley, Verint Systems vende centros de monitoreo que "posibilitan la interceptación, monitoreo y análisis de comunicaciones específicas y masivas prácticamente en cualquier red" y que, según el sitio web de la empresa, se utilizan en más de 75 países.[47]

Verint Systems es conocida por suministrar tecnología de vigilancia a gobiernos donde la vigilancia de las comunicaciones y la represión política son generalizadas, como Kazajistán y Uzbekistán, donde, como ha revelado Privacy International, los activistas, periodistas, abogados y políticos considerados contrarios al gobierno son objeto de estricto monitoreo.[48]

La empresa describe sus centros de monitoreo señalando que están divididos en dos áreas funcionales: un back-end o parte trasera formada por el centro de monitoreo en sí, donde los analistas solicitan y reciben datos, un front-end o parte delantera situada dentro de la red de telecomunicaciones y que intercepta los datos antes de enviarlos al centro de monitoreo.[49] Si se hace una solicitud de datos en el centro de

43 "In a Faded Wall St. Scandal, Lessons for a Current One", Solomon, S, 26 de marzo de 2013, http://dealbook.nytimes.com/2013/03/26/in-a-faded-wall-st-scandal-lessons-for-a-current-one/?_r=0

44 Bamford, James, "The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America", 2008, Knopf Doubleday Publishing Group.

45 "Verint Announces Fourth Quarter and Full Year Results" Verint, 31 de marzo de 2014, http://www.verint.com/assets/verint/documents/january-31-2014-earnings-press-release-exhibit-99%201_3_31_14.pdf?_ga=1.84395997.57461801.1410275227

46 "For sale: Systems that can secretly track where cellphone users go around the globe" Timberg, Craig, The Washington Post, agosto de 2014, http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

47 "Verint to supply new Swiss spying system", Swiss Info, 15 de enero de 2014, http://www.swissinfo.ch/eng/verint-to-supply-new-swiss-spying-system/37740006

48 "Private Interests: Monitoring Central Asia", Privacy International, noviembre de 2014, https://www.documentcloud.org/documents/1381566-12-dec-private-interests-updated.html

49 "Verint Selected To Provide Law Enforcement Communications Interception Solution To A New Customer In Asia Pacific", Verint, julio de 2002, http://phx.corporate-ir.net/phoenix.zhtml?c=131043&p=irol-newsArticle_print&ID=312250&highlight=

monitoreo, la parte delantera correspondiente del sistema situada en la red responde interceptando los datos y enviándolos a la parte trasera.

Desde 2005, la empresa ha desempeñado un papel esencial en el desarrollo de las capacidades de interceptación masiva de Colombia, facilitado por su representante local y proveedor exclusivo, La Curacao. Los técnicos de Verint Systems se ocuparon de la configuración inicial del sistema, mientras que los de La Curacao se encargaron del mantenimiento preventivo y correctivo y de la formación de los agentes de la Policía en su uso.

A través de La Curacao, Verint Systems suministró también una sonda de red al DAS en algún momento, antes de 2011. Incluso en agosto de 2011, cuando estaba siendo ya investigado por interceptaciones ilegales y faltaban dos meses para que fuera disuelto oficialmente, el DAS pagó para que La Curacao garantizara "el pleno funcionamiento e integridad de la solución sistema de la sala de análisis de información registrada al navegar por Internet REUANT de Verint@ System".[50] Este servicio incluía mantener la "sonda táctica en cualquier lugar del país donde se encuentre operando", lo que indica que era una sonda que podía quitarse y volverse a insertar para intervenir cables cuando fuera necesario. La embajada de Estados Unidos en Bogotá también contrató a la rama estadounidense de Verint Systems para el "mantenimiento y soporte" de su sala de interceptación.[51]

NICE Systems, Eagle Commercial y la ampliación de PUMA

En 2013, la policía colombiana se propuso ampliar la capacidad de interceptación de PUMA. La empresa israelí de tecnología NICE Systems, en unión con la colombiana Eagle Commercial, consiguió la adjudicación de un contrato de 26 millones de dólares estadounidenses (50.000 millones de pesos colombianos) para ampliar la plataforma.

La ampliación de PUMA habría dado a la Policía capacidad para interceptar 20.000 "objetos", con la posibilidad de aumentar su número a 100.000. "Súper-PUMA" exhibía también capacidades nuevas, como un módulo de monitoreo para tráfico de ISP y hasta 700 estaciones de trabajo por todo el país.[52] Los datos serían interceptados por medio de ocho sondas "NiceTrack IP", que "filtran y extraen cantidades inmensas de datos enviados simultáneamente a través de sobrecargados enlaces IP".[53] Por primera vez en la historia de los sistemas conocidos de interceptación de Colombia, el sistema sería capaz de interceptar datos 4G.

50 "Contrato de Prestación de Servicios de 2011, Celebrado entre el Fondo Rotatorio del Departamento Administrativo de Seguridad DAS Y Compañía Comercial Curacao de Colombia S.A.", Fondo Rotatorio del Departamento Administrativo de Seguridad, 22 de agosto de 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-620217

51 "List Of Contract Actions Matching Your Criteria: Verint, State Department, American Embassy Bogota", Sistema de Datos sobre la Contratación Pública de Estados Unidos (USFPDS), 20 de abril de 2015, https://www.fpds.gov/ezsearch/fpdsportal?s=FPDSNG.COM&q=VERINT+DEPARTMENT_FULL_NAME%3A%22STATE%2C+DEPARTMENT+OF%22+CONTRACTING_OFFICE_NAME%3A%22AMERICAN+EMBASSY+-+BOGOTA+-+GSO%22&indexName=awardfull&y=0&templateName=1.4.4&x=0

52 "Asunto: Respuesta proposición N.04 de 2013", Policía Nacional de Colombia, 12 de agosto de 2013

53 "NiceTrack™ Passive Interception for Packet Data and VoIP Networks", NICE Systems, 2007, http://www.nice.com/ru/files/IP_2007.pdf

Fabricante originalmente de productos de vigilancia sólo para usuarios militares, NICE Systems dice ser en la actualidad "líder mundial en soluciones basadas en la intención que captan y analizan interacciones y transacciones, hacen efectiva la intención y extraen e impulsan percepciones para causar impacto en tiempo real".[54] Fundada por siete miembros del ejército israelí,[55] la empresa está radicada en Israel, aunque sus participaciones cotizan también en el NASDAQ estadounidense.

NICE Systems tiene tres ramas principales. NICE Enterprise se especializa en centros de llamadas y productos conexos, como análisis de big data y análisis de voz. NICE Actimize está especializada en soluciones analíticas para instituciones financieras con que satisfacer los requisitos de cumplimiento de la normativa financiera, incluidas la normas contra el banqueo de dinero. NICE Security ofrece soluciones de vigilancia basada en vídeo y análisis conexo, así como tecnologías de vigilancia electrónica, incluidas herramientas de interceptación de telefonía vía satélite. Los centros de monitoreo de NICE Systems que se ofrecen incluyen capacidades para interceptar a escala masiva datos IP, móviles y de teléfono y un centro de rastreo de ubicación que permite a los usuarios "localizar a cualquiera, en cualquier momento y en cualquier lugar" por medio de teléfonos móviles.[56] NICE Systems comercializa también varios componentes analíticos más, que pueden utilizarse en un centro de monitoreo, como Pattern Analyzer, que sirve para "identificar irregularidades de conducta que puedan apuntar a actividades delictivas o terroristas".[57]

Junto con Verint Systems, NICE Systems es conocida por suministrar tecnología de vigilancia a gobiernos donde la vigilancia de las comunicaciones y la represión política son generalizadas, como Kazajistán y Uzbekistán, donde, como ha revelado Privacy International, los activistas, periodistas, abogados y políticos considerados contrarios al gobierno son objeto de estricto monitoreo.[58] NICE Systems enumera a unas 25.000 organizaciones de más 150 países en su lista de clientes, y en 2013 declaró unos ingresos totales de 951 millones de dólares estadounidenses.[59] En mayo de 2015, la empresa israelí de tecnología de defensa Elbit Systems Limited firmó un acuerdo de adquisición del departamento de ciberinteligencia de NICE System.[60]

54 "Company Overview", NICE Systems, 2015, http://www.nice.com/company-overview

55 "NICE News Special Edition, vol. 2 iss. 3", NICE Systems, marzo de 2006, http://www.nice.com/news/newsletter/6_03s/anniversary.php

56 "Location Tracking", NICE Systems, 2015, http://www.nice.com/intelligence-lea/location-tracking

57 "Pattern Analyzer", NICE Systems, 2015 http://www.nice.com/intelligence-lea/pattern-analyzer

58 "Private Interests: Monitoring Central Asia", Privacy International, noviembre de 2014, https://www.documentcloud.org/documents/1381566-12-dec-private-interests-updated.html

59 "NICE Reports Record Revenues and EPS for the Fourth Quarter and Full Year 2013", NICE Systems, 5 de febrero de 2014, http://www.nice.com/nice-reports-record-revenues-and-eps-fourth-quarter-and-full-year-2013

60 "Elbit Systems Signs an Agreement to Acquire NICE Systems Cyber and Intelligence Division for an Amount of Up to $157.9 Million", Elbit Systems Limited, 21 de mayo de 2015, http://ir.elbitsystems.com/phoenix.zhtml?c=61849&p=irol-newsArticle&ID=2052104

El socio colombiano de NICE Systems es Eagle Commercial SA. Como con STAR, Eagle Commercial tiene tratos comerciales con el DAS, la Policía, las Fuerzas Armadas y la Embajada de Estados Unidos, entre otros clientes. Representa también a varios clientes internacionales, como American Harris Corporation, y ha entablado una nueva relación de distribución con Taser International Inc., fabricante de material electrónico paralizante.[61] En 2010 declaró unos beneficios de más de 470 millones de dólares estadounidenses después de impuestos.[62]

Intereses rivales

En el mercado de la interceptación legal, Verint Systems y Nice Systems están consideradas como rivales,[63] pese a que a principios de 2013 se rumoreó que la segunda estaba negociando la compra de aquélla.[64] Sus socios colombianos respectivos, La Curacao e Eagle Commercial, también son rivales y han competido en licitaciones para contratos de vigilancia.[65]

La Curacao se esforzó mucho por conseguir un contrato en exclusividad para el mantenimiento del sistema PUMA. De hecho, el especialmente lucrativo contrato de la ampliación de PUMA degeneró en una encarnizada batalla legal entre los dos gigantes y sus representantes colombianos. La Curacao disfrutaba de contratos exclusivos por valor de al menos 5.000 millones de pesos (2 millones de dólares estadounidenses) adjudicados por contratación directa, es decir, sin que el organismo contratante (la Policía, en este caso) elija al contratista tras convocatoria pública.[66] Pero, cuando, en 2010, La Curacao escribió a la Policía para decirle que se le debía adjudicar un contrato directo a fin de evitar que "personas sin formación" que no conocen el "altamente sofisticado y complejo sistema de Verint Systems causen más daños en él", La Policía respondió que no tenía ninguna obligación de contratar en exclusividad a la empresa.[67]

61 "Importador de inteligencia", El Espectador, 27 de marzo de 2011, http://www.elespectador.com/noticias/wikileaks/importador-de-inteligencia-articulo-259259

62 "Importador de inteligencia", El Espectador, 27 de marzo de 2011, http://www.elespectador.com/noticias/wikileaks/importador-de-inteligencia-articulo-259259

63 "Verint Watches You, Should You Watch It?", Investopedia, 5 de septiembre de 2012, http://www.investopedia.com/stock-analysis/2012/verint-watches-you-should-you-watch-it-vrnt-cmvt-nice-hpq0910.aspx and "Verint overtakes Nice to snatch Witness in a surprise move", Haaretz, 13 de febrero de 2007, http://www.haaretz.com/print-edition/business/verint-overtakes-nice-to-snatch-witness-in-a-surprise-move-1.212838

64 "Nice Systems in talks to buy Verint-report", Reuters, 14 de enero de 2013, http://www.reuters.com/article/2013/01/14/nicesystems-verint-idUSL6N0AJ5GV20130114

65 "Acta No.070 2006: Contratación Directa No. 057 de 2006", Fondo Rotatorio de la Policía, Ministerio de Defensa Nacional, 3 de noviembre de 2006.

66 "Infografía: La Contratación Directa en Colombia", Kontrato.co, 5 de agosto de 2013, http://blog.kontrato.co/blog/2013/08/05/infografia-la-contratacion-directa-en-colombia/

67 "Asunto: "Respuesta observaciones: Actualización y Mantenimiento Plataforma PUMA", Dirección Administrativa y Financiera, 30 de marzo de 2010, http://www.contratos.gov.co/archivospuc1/2010/ACL/116001000/10-9- 120274/ACL_PROCESO_10-9-120274_116001000_1656021.pdf (archivado)

Cuando NICE-Eagle consiguió el contrato de ampliación de PUMA en marzo de 2013, La Curacao devolvió el golpe. En una carta a la Secretaría para la Transparencia, el abogado de La Curacao[68] presentó pruebas de que NICE Systems habían falsificado los diplomas de sus técnicos. Meses más tarde, La Curacao fue acusada en una denuncia ante la Contraloría General de haber sobornado al coronel Jairo Gordillo Rojas, ex director telemático de la Policía Nacional, durante el proceso de contratación de PUMA, invitándolo, por ejemplo, a viajes de negocios a Europa con todos los gastos pagados.[69] El propio Gordillo había sido interrogado ese mismo año acerca de la interceptación ilegal de llamadas de teléfono de periodistas.[70]

La decisión de elegir a NICE Systems en vez de a Verint Systems se debió con toda probabilidad a rivalidades entre contratistas del sector de defensa que intentaban ofrecer sus productos a un gobierno cada vez más impaciente por probar resultados, y para los que el contrato de PUMA era especialmente lucrativo, según personas que siguieron de cerca el proceso.[71] Cualquiera que fuera el motivo, la preocupación por la posible corrupción ensombreció el debate en los medios de comunicación sobre simplemente cuán potente sería el nuevo "Súper-PUMA".

INTERCEPTACIÓN POR TODAS PARTES

(Reverso)

LISTA INVITADOS PENLINK

ENTIDAD	DPTO		NOMBRE
FISCALIA	CONTROL TELEMATICO	1	PILAR VAQUERO
		2	JAIME CHACON
		3	TEDDY DUQUE
	INFORMATICA FORENSE	4	
		5	
DAS	DGO	6	CARLOS ALVAREZ
		7	NELSON BETANCOURT
		8	CARLOS MARIO
		9	
	DESARROLLO TECNOLOGICO	10	MARCO ANTONIO CRUZ
		11	RAMIRO ORDOÑEZ
POLICIA		12	LUIS VARGAS VALENCIA
		13	HENRY SANABRIA
		14	JAIRO GORDILLO
		15	CAROLINA IBAGUE
DIJIN		16	MAYOR LEON
		17	
		18	
SIJIN		19	
		20	
ARMADA		21	CESAR AUGUSTO NARVAEZ
		22	
EJERCITO		23	JUAN GILBERTO VALENCIA
		24	ALVARO AUGUSTO VALLEJ
		25	MARTIN FERNANDO NIETO
		26	OSCAR MAURICIO COTE
		27	DANILO SAAVEDRA

68 "Contratos por más de US 35 millones para renovar salas de interceptación", Radio Caracol, 25 de abril de 2014, http://www.caracol.com.co/noticias/judiciales/contratos-por-mas-de-us-35-millones-para-renovar-salas-de-interceptacion/20140425/nota/2194095.aspx

69 "Las denuncias de corrupción contra el general León Riaño y sus hermanos", La F.M., 21 de marzo de 2014, http://www.lafm.com.co/noticias/las-denuncias-de-corrupcion-157475#ixzz3XqkMcdLm

7o "Fiscalía realiza interrogatorios por supuestas 'chuzadas'", Noticias RCN, 9 de mayo de 2014, http://www.noticiasrcn.com/nacional-pais/fiscalia-realiza-interrogatorios-supuestas-chuzadas

71 El 30 de marzo de 2010, la DIJIN respondió a la queja de La Curacao. Señaló que no estaba obligada a contratar únicamente a La Curacao y mencionó la necesidad de transparencia en el proceso de selección.

INTERCEPTACIÓN POR TODAS PARTES

Bogotá D.C., Julio 17 de 2009

Señor Teniente Coronel:
Luis Vargas Valencia
Dirección de Inteligencia Policial
Ciudad

En nombre de Pen-Link Ltd y nuestros asociados en Colombia – STAR Inteligencia & Tecnología, lo invitamos cordialmente a participar en nuestra Conferencia para Latino América, la cual se llevará a cabo los días 10- 11 y 12 de Agosto, en el Hotel Sheraton, ubicado en la Avenida el Dorado No. 69 C 80.

El propósito de la Conferencia es mostrar los avances que se han tenido en el Área de Interceptación Legal a nivel técnico y de métodos, con el objetivo de llevar a cabo procesos adecuados en búsqueda de garantizar la seguridad de los ciudadanos y del Estado. Su experiencia y conocimiento en ésta área son particularmente invaluables.

Esperamos poder contar con su presencia tanto en las sesiones generales como en una reunión privada donde se podrá discutir abiertamente la forma como Pen-Link puede apoyar efectivamente a las agencias responsables para realizar Interceptación legal. Conscientes de sus múltiples ocupaciones y con el propósito de ajustar el horario de la reunión privada, le solicitamos nos informe la hora que más se ajusta a su agenda a fin de atenderlo como bien se merece, le agradecemos si esta verificación la realiza por intermedio de STAR Inteligencia & Tecnología.

Cordialmente,

OSCAR ALIRIO REYES CASTRO
Gerente General
STAR I&T S.A.

Av El Dorado No 68C 61 Oficina 327-3
PBX: +57 (1) 427 5077
www.star-colombia.com
Nit 830.139.912-1
e-mail: star@star-colombia.com
FAX: +57 (1) 427 5076

STAR invitó a miembros del DAS, la Policía (la DIPOL y la DIJIN), la Armada y el Ejército en su calidad de representantes de “las agencias responsables para realizar Interceptación legal “, además de la Fiscalía, a un acto promocional celebrado en el hotel Sheraton en 2008. Pen-Link celebró un acto de apariencia promocional, acto, en el que no faltó la indumentaria promocional para representantes de organismos como el DAS, la DIPOL y la Central de Inteligencia Técnica (CITEC) del Ejército, a los que se invitó a presenciar demostraciones de los productos de la empresa, además de mostrarles los avances realizados en el área de la interceptación legal.

Otras empresas europeas

También han comercializado y vendido productos de interceptación de redes a las autoridades colombianas otras empresas. La relación entre estos productos y los sistemas existentes anteriormente descritos no está clara.

La empresa estadounidense de tecnología de interceptación Network Critical ofreció puntos de acceso de tráfico (TAP) pasivos de fibra óptica a la DIPOL (véase el anexo). No se sabe bien qué relación guardan con el programa de vigilancia existente de la DIPOL, el Sistema Integral de Grabación Digital.

Network Critical produce "controladores de visibilidad de red" y es la creadora de la solución de TAP de redes.[72] En el sector privado, tales tecnologías, conocidas también como sniffers ("olfateadores") de red,[73] pueden ayudar a las empresas a detectar fugas de datos y monitorear cómo los visitantes participan en sus sitios. Como estas técnicas analizan y monitorean el tráfico, son apropiadas como tales para la vigilancia electrónica, y se utilizan ampliamente para ello y con fines de censura en todo el mundo. Los productos TAP SlimLine ofrecidos a la DIPOL están concebidos para mejorar el rendimiento del centro de monitoreo permitiendo el acceso al tráfico de red activo y proporcionando copias del flujo de datos a puertos de monitoreo separados en el centro.[74] SlimLine es compatible con los productos de interceptación de varios vendedores, incluida Verint Systems.[75]

La empresa neerlandesa de tecnología de interceptación Digivox también vendió puntos de acceso de tráfico de red en Colombia. Digivox es una empresa radicada en Rotterdam, que desarrolla y vende material de interceptación de comunicaciones IP y telefónicas. En 2008, STAR elaboró presupuestos para puntos de acceso de tráfico de red ComLog de Digivox. Su sistema de gestión de puntos de acceso de tráfico permite la programación centralizada de switches IP y de telecomunicaciones a escala nacional con fines de interceptación legal. Comlog puede conectar líneas interceptadas con, por ejemplo, los teléfonos móviles de agentes investigadores en tiempo real.[76]

72 "Network Critical is the Preferred TAP Solution for Use with the Enterasys Intrusion Prevention System (IPS).", Network Critical, 15 de septiembre de 2010, https://networkcritical.wordpress.com/2010/09/15/network-critical-is-the-preferred-tap-solution-for-use-with-the-enterasys-intrusion-prevention-system-ips/

73 "Network Critical" Sourcefire, 2015, http://www.sourcefire.com/partners/technology-partners/sourcefire-technology-partners/network-critical

74 "Passive Taps", Network Critical, 2015, http://www.networkcritical.com/products/passive-taps

75 "Lawful Interception Deployments", Network Critical, 2011, http://www.networkcritical.com/NetworkCritical/media/resource-library/other/Network-Critical-Solution-Deployment-Lawful-Interception.pdf

76 "Comlog", Digivox, 2015, http://www.digivox.nl/comlog/Comlog_English.htm

Interceptación táctica

Las tecnologías de interceptación táctica son herramientas de vigilancia que recopilan datos de comunicaciones interceptadas de manera inalámbrica o directamente de un dispositivo específico, no de la arquitectura de red del proveedor de servicios. Pueden transportarse con facilidad a lugares distintos para su utilización. Las tecnologías como los IMSI catchers[77] y las herramientas de intrusión[78] están presentes en Colombia, y las utilizan distintos organismos del Estado.

Las empresas: Interceptación táctica

Muchas empresas internacionales y nacionales han suministrado productos de interceptación táctica a los organismos colombianos de inteligencia y encargados de hacer cumplir la ley. Entre las que han competido para vender tales productos a la Policía y al DAS figuran Spectra Group y Smith Myers, que tienen su sede en el Reino Unido. Los agentes del DAS utilizaban software de la empresa estadounidense AccessData en unidades forenses móviles con las que se podían conseguir datos privados directamente de dispositivos específicos. Finalmente, la Policía ha hecho negocios con Hacking Team, empresa de tecnología radicada en Italia y conocida sobre todo por el malware ofensivo que produce, que básicamente permite hackear y controlar a distancia dispositivos específicos.

Uno de los productos de interceptación táctica más comunes son los IMSI catchers, conocidos también como stingrays en Estados Unidos.[79] Los dispositivos móviles se identifican por dos números exclusivos: la identidad internacional del abonado móvil (IMSI), que identifica la tarjeta SIM del abonado, y la identidad internacional del equipo móvil (IMEI), que identifica el dispositivo real. Ambos números se comunican de manera habitual a los proveedores de servicios de red a medida que el usuario se desplaza de un sitio a otro. Ciertas tecnologías de monitoreo de ubicación identifican la actividad correspondiente a estos dos números que el organismo que lleva a cabo el monitoreo pueda considerar sospechosa, como el cambio de la tarjeta SIM (es decir que se mantenga el número IMEI pero el número IMSI cambie a menudo).

Los IMSI catchers son dispositivos de monitoreo que transmiten una potente señal inalámbrica que hace que los teléfonos de los alrededores se conecten a ellos y trasmitan datos y contenido de las comunicaciones. Pueden actualizarse con tecnologías de monitoreo de ubicación que determinan la ubicación de un objetivo con una precisión de un metro. Estos dispositivos pueden "apuntarse" al dispositivo

77 "Phone Monitoring", Surveillance Industry Index, 2015, https://www.privacyinternational.org/sii/technologies/phone-monitoring

78 "Phone Monitoring", Surveillance Industry Index, 2015, https://www.privacyinternational.org/sii/technologies/phone-monitoring

79 "Florida Cops' Secret Weapon: Warrantless Cellphone Tracking", Wired, 3 de marzo de 2014, http://www.wired.com/2014/03/stingray/

de una persona en particular, dirigiéndolos, por ejemplo, a su lugar de trabajo, pero también pueden utilizarse para identificar a personas desconocidas que asistan a manifestaciones u otras reuniones, porque se conectarán al IMSI catcher tantos teléfonos móviles como el sistema pueda acoger.

En Colombia ofrecen IMSI catchers muchas empresas. En septiembre de 2005, Spectra Group, radicada en el Reino Unido, suministró su IMSI catcher Laguna a la DIPOL a través la empresa colombiana Maicrotel Ltda. El sistema Laguna sirve para monitorear y grabar conversaciones telefónicas y datos de sistemas de comunicaciones móviles y puede ser portátil o ir montado en estaciones fijas.[80] Bulldog y Nesie, fabricados por la empresa británica de vigilancia Smith Myers, son otros dos populares IMSI catchers vendidos en Colombia. En 2010, el DAS se dispuso a comprar un sistema de interceptación Bulldog por más de 250.000 dólares estadounidenses y un sistema Nesie por más de 320.000. La Fiscalía también tenía pensado comprar un sistema Bulldog por algo más de 280.000 dólares estadounidenses, al igual que la Seccional de la DIJIN de Bogotá. En 2014, la rama finlandesa de la empresa canadiense de telecomunicaciones Exfor exportó su IMSI catcher NetHawk F10 a Colombia.

Otra forma de interceptación táctica es el rastreo por GPS, que utiliza las señales de telefonía móvil. Aunque no interceptan el contenido de las llamadas telefónicas, estas tecnologías permiten el rastreo detallado de los dispositivos por las señales que emiten. STAR presentó el GSM Tracking System de la empresa finlandesa de infraestructura de telecomunicaciones Nokia a la Escuela de Inteligencia del Ejército, que le habría permitido rastrear a personas utilizando teléfonos móviles con GPS activado en tiempo real. TAMCE, empresa radicada en México y con una oficina en Bogotá,[81] ofrece varias herramientas de rastreo por GPS, así como un IMSI/IMEI catcher 3G.[82]

80 “Contrato de Compraventa No. 152 de 2005, celebrado entre el Fondo Rotatorio de la Policía y la Firma M@icrotel LTDA.”, Fondo Rotatorio de la Policía, 30 de septiembre de 2005.

81 “GPS Logger”, TAMCE, 2015, http://tamce.net/categorias/71/gps_logger

82 “3G IMSI/IMEI Catcher”, TAMCE, 2015, http://mobile.tamce.net/productos/902/3g_imsi_imei_catcher

En un contrato de 2006, las empresas licitadoras tuvieron que demostrar las capacidades de sus productos interceptando los teléfonos de unos objetivos en determinados lugares de Bogotá, como el Centro Comercial Calle 80, al que corresponde esta fotografía.[83]
Créditos: Privacy International (2014)]

83 “Adjudicación de la Contratación Directa No. 055 de 2006”, Fondo Rotatorio de la Policía, Ministerio de Defensa Nacional, 29 de noviembre de 2006, https://www.contratos.gov.co/archivospuc1/ADA/115001003/06-2-16355/ADA_PROCESO_06-2-16355_115001003_31717.pdf (archivado)

ARTÍCULOS POPULARES

El producto Bulldog de la empresa británica de vigilancia Smith Myers simula ser un emplazamiento de estación base de telefonía móvil para conectarse con los móviles de una zona específica y recopilar su información de identificación (IMSI, TMSI e IMEI). Equipado con sistemas de radiogoniometría, Bulldog localizará dispositivos específicos y a sus usuarios entre muchos otros dispositivos en una zona determinada. Nesie, otro producto de Smith Myers, también obtiene la información de identificación de los teléfonos móviles de la zona simulando ser un emplazamiento de estación base móvil. Puede negar el acceso de teléfonos específicos a la red real, obligándolos a conectarse con él y comunicar el contenido de llamadas no cifradas en tiempo real a los operadores de Nesie.

También pueden conseguirse las comunicaciones de una persona físicamente desde su dispositivo. Por ejemplo, un agente podría copiar con fines forenses los datos de comunicaciones contenidos en un dispositivo retenido de manera encubierta o en el momento de la detención de una persona. En julio de 2007, el DAS publicó las especificaciones técnicas de un concurso para la adquisición de equipos que le permitirían copiar e inspeccionar los dispositivos de sus objetivos. Aunque al final se canceló la licitación en diciembre de 2006, el DAS adquirió la tecnología antes de 2010. La Curacao consiguió un contrato de mantenimiento compitiendo con Internet Solutions Ltda. y SF International. El software utilizado por el DAS era Forensic Toolkit (FTK), conjunto de programas de informática forense de la empresa radicada en Estados Unidos AccessData. El software 3.0 FTK especificado en el contrato de 2010 permite a un analista no sólo "prever la máquina de un objetivo desde el otro lado de la red para determinar la pertinencia antes de la adquisición, sino [...] también adquirir y analizar completamente los datos contenidos en el sistema, incluida la RAM

[memoria de acceso aleatorio]".[84] Una función de accionamiento remoto permite a los analistas analizar desde su sistema con fines forenses los datos activos –como la memoria del sistema, los volúmenes lógicos y los dispositivos físicos– en un dispositivo remoto. El software podría también utilizarse para desencriptar discos encriptados con PGP.[85]

El malware ofensivo es una herramienta de vigilancia especialmente invasiva, que se utiliza contra dispositivos conocidos. Puede atacar al objetivo instándole a que permita al software instalarse en él, por medio, por ejemplo, de falsas actualizaciones de seguridad o descargas aparentemente inocuas. Una vez instalado, el malware ataca y explota la memoria y el sistema operativo del dispositivo, permitiendo que un analista controle éste a distancia. El software de intrusión o malware se comercializa por lo general como necesario para cubrir un presunto vacío entre la interceptación pasiva (como el monitoreo de redes) y las búsquedas físicas, permitiendo el acceso directo de terceros a los datos almacenados, enviados y recibidos de un dispositivo específico infectado. Este tipo de material puede estar integrado en los centros de monitoreo de organismos específicos y ser utilizado directamente por los organismos de inteligencia y encargados de hacer cumplir la ley. Las empresas que fabrican estas tecnologías exhiben periódicamente sus productos en ferias de vigilancia y seguridad. El uso de tecnologías de intrusión es ilegal y no está previsto en la legislación colombiana.[86]

Hacking Team produce un sistema de intrusión que fue adquirido por la policía colombiana. Su Remote Control System (RCS) puede utilizarse para interceptar ordenadores y dispositivos móviles sin que los usuarios lo detecten, pues está concebido de manera que burle la encriptación y los programas antivirus corrientes. Infectando el dispositivo del objetivo, la suite RCS puede recopilar datos de él, activar y desactivar a distancia la webcam y el micrófono y copiar archivos y contraseñas tecleadas. En 2014, Hacking Team tenía un técnico externo en Colombia y un contrato activo con la policía colombiana. Se sospechaba del uso por parte el gobierno colombiano de productos de malware ofensivo de Hacking Team desde que los investigadores de The Citizen Lab identificaron un servidor de comando y control para la suite RCS en el país.[87] Hacking Team suministró su tecnología a la DEA, que, según mensajes internos de correo electrónico, utilizó el software espía para llevar a cabo actividades de vigilancia desde la embajada de Estados Unidos en Bogotá.[88] Hacking Team tuvo también dos proyectos con la policía colombiana, uno de ellos relacionado con el sistema de vigilancia PUMA.[89]

84 "AccessData Releases Forensic Toolkit® 3.0", AccessData, 22 de septiembre de 2009, https://ad-pdf.s3.amazonaws.com/FTK3_press_release.pdf

85 La desencriptación se haría buscando las claves de encriptación en el dispositivo, no rompiéndolas. "AccessData FTK 3.0.4 Release Notes", AccessData, 2009, https://ad-pdf.s3.amazonaws.com/ftk3-0-4readme.pdf

86 Sin embargo, la empresa colombiana Emerging Technologies Corporation dice vender "soluciones de intrusión remota para PCs". "Inteligencia de Señales", Emerging Technologies Corporation, 2015, http://etcsa.com/sistemas-de-informacion-e-inteligencia/inteligencia-de-senales/

87 "Mapping Hacking Team's 'Untraceable' Spyware", The Citizen Lab, 17 de febrero de 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

88 "Hacking Team emails expose proposed death squad deal, secret U.K. Sales push and much more", The Intercept, 9 de julio de 2015, https://firstlook.org/theintercept/2015/07/08/hacking-team-emails-exposed-death-squad-uk-spying/

89 "El software espía de la Policía", El Espectador, 11 de julio de 2015, http://www.elespectador.com/noticias/investigacion/el-software-espia-de-policia-articulo-571980

Conclusión

La industria de la vigilancia es la savia que nutre las actividades de vigilancia de los Estados en todo el mundo. Empresas como Verint Systems, NICE Systems, Pen-Link, Komcept, Hacking Team y sus socios colombianos, como STAR, Eagle Commercial y La Curacao, facilitan la vigilancia estatal. Son, por tanto, responsables en cierto modo de la legalidad de sus actividades y de las consecuencias que tienen en los derechos humanos. Las empresas que suministran sistemas de vigilancia masiva directamente posibilitan la vigilancia desproporcionada e indiscriminada, en contra de los principios de derechos humanos internacionalmente establecidos

Apenas unas cuantas personas pertenecientes a la industria parecen haber tenido debidamente en cuenta las consecuencias de sus actividades en los derechos humanos. Es así a pesar de los considerables datos que indican que la industria está teniendo consecuencias negativas en el disfrute de los derechos humanos en todo el mundo.

En vez de reconocer sus responsabilidades, las empresas tienden más bien a echar la culpa y responsabilizar del uso indebido de las tecnologías de vigilancia al usuario final de los productos y servicios que suministran. Esta actitud va en contra de principios establecidos que regulan la responsabilidad de las empresas de respetar los derechos humanos. El hecho de que un Estado viole los derechos humanos no exime en modo alguno a una empresa de la responsabilidad de respetarlos. En las circunstancias en que la venta de tecnología pueda dar lugar abusos contra los derechos humanos, esa responsabilidad es aún mayor.

Indudablemente, para conocer las consecuencias de la industria de la vigilancia en los derechos humanos es condición necesaria que haya mayor transparencia. Con información limitada, a las organizaciones de la sociedad civil les resulta sumamente difícil hacer rendir cuentas a las empresas de vigilancia por los abusos contra los derechos humanos. Es responsabilidad de las empresas no sólo ser más transparentes, sino también conocer bien las consecuencias de sus actividades en los derechos humanos y tomar medidas para prevenir los abusos contra los derechos humanos provocados por el uso de los productos y servicios que suministran a los Estados.

El medio principal por el que las empresas pueden limitar los efectos perjudiciales del uso de sus productos y servicios en los derechos humanos consiste en garantizar que no participan activamente en el desarrollo de las capacidades de vigilancia de los países si su uso va ligado a injerencias en los derechos humanos, los principios democráticos o la libertad de expresión. Además, los Estados deben aplicar medidas de control de las exportaciones a la venta de tecnologías de vigilancia a organismos de inteligencia y encargados de hacer cumplir la ley de Estados con un historial deficiente en materia de derechos humanos. Estas medidas de control deben conformarse atendiendo a estrictos criterios basados en los derechos humanos, a fin de garantizar que las empresas que están dentro de la jurisdicción de los Estados no exportan a usuarios finales con los que se corra el riesgo de que la transferencia represente una amenaza para los derechos humanos.

Anexo 1

XXXXXXXXXXX

STAR Inteligencia & Tecnología	**FORMATO DE COTIZACIÓN** **STAR INTELIGENCIA & TECNOLOGÍA**	VERSION :1 CODIGO: GC-FO-47 FECHA DE APROBACION: 28 DE MAYO 2010

Señores:	POLICÍA NACIONAL MEBOG SIJIN
Contacto:	Sr. Mayor Campo Elías Vasquez Rojas
Dirección:	
Telefóno:	
E-mail:	
Fecha:	22/07/2010
Ciudad:	Bogotá DC

GC-169-Cotización

OFERTA BÁSICA BUSINESS

ITEM	REF.	DESCRIPCION	CANT.	UND.	VR. UNITARIO	VALOR TOTAL
1	S&M	**Sistema de monitoreo pasivo para redes IDEN (Avantel) de 12 canales "Nesie".**	1	UND.	$ 554.182.238	554.182.238
2	S&M	**Equipo de radio goniometría (DF) para montaje en vehículo DF10i**	1	UND.	$ 189.136.315	189.136.315
					SUBTOTAL	**743.318.554**
					IVA (16%)	**118.930.969**
					TOTAL	**862.249.522**

CONDICIONES COMERCIALES	
MONEDA DE LA OFERTA	Pesos Colombianos
VALIDEZ DE LA OFERTA	30 días
TIEMPO DE ENTREGA	A convenir
FORMA DE PAGO	50% de anticipo; 30% contra notificación de embarque; 20% contra entrega a satisfacción.
GARANTIA	12 meses
OBSERVACIONES	Estos bienes están exentos de IVA. Literal d) del estatuto tributario, concepto 06094 de 1999 y concepto unificado 003/2003 de la DIAN. Este equipo demodula audio.

Elaboró: Jaime Chacón
Aprobó: Rodrigo Priast
Cargo: Gerente Comercial

Anexo 2

XXXXXXXXXXX

STAR Inteligencia & Tecnología	**FORMATO DE COTIZACIÓN** **STAR INTELIGENCIA & TECNOLOGÍA**	VERSION :1 CODIGO: GC-FO-47 FECHA DE APROBACION: 28 DE MAYO 2010

Señores:	DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS
Contacto:	Ing. Ramiro Ordoñez
Dirección:	Carrera 27 # 17A - 00
Telefóno:	408 80 00 Ext. 2108
E-mail:	coordinacioncienciaytecnologia@das.gov.co
Ciudad:	Bogotá DC

GC-151-Cotización

ITEM	REF.	DESCRIPCION	CANT.	UND.	VR. UNITARIO	VALOR TOTAL
1	BLDG	**Kit analizador de espectro y sistema de goniometría para ingeniería de redes móviles. Incluye los siguientes componentes: receptor panorámico 824 - 894 MHz "Bulldog" (1); goniómetro móvil HHDF (1)**	1	UND.	$ 483.350.582	483.350.582
					SUBTOTAL	**483.350.582**
					IVA	
					TOTAL	**483.350.582**

CONDICIONES COMERCIALES	
MONEDA DE LA OFERTA	Pesos Colombianos
VALIDEZ DE LA OFERTA	30 días
TIEMPO DE ENTREGA	A convenir
FORMA DE PAGO	50% de anticipo; 30% contra notificación de embarque; 20% contra entrega a satisfacción.
GARANTIA	12 meses
OBSERVACIONES	Estos bienes pueden estar exentos de IVA. Literal d) del estatuto tributario, concepto 06094 de 1999 y concepto unificado 003/2003 de la DIAN.

Elaboró:	Rodrigo Priast
Aprobó:	Rodrigo Priast
Cargo:	Gerente Comercial

Anexo 3

XXXXXXXXXXX

Bogotá D.C. Abril 16 de 2009

SEÑORES:
DIRECCION DE INTELIGENCIA POLICIAL DIPOL
Ciudad

GG-RE- 025

Por medio de la presente estamos haciendo entrega de los siguientes elementos relacionados a continuación, correspondientes al contrato No. 06-2-10559-078, celebrado entre la POLICIA NACIONAL y STAR INTELIGENCIA Y TECNOLOGIA

ITEM	DESCRIPCION	No. SERIAL
FO-M17001-LC	Slimline Fiber Optic Passive TAP 70:30 MMF 62.5pm,850/131nm,LC	0809F0323
FO-M37001-LC	Slimline Fiber Optic Passive TAP 70:30 MMF 50pm, OM3, 850/131nm,LC	71220066163
FO-S17001-LC	Slimline Fiber Optic Passive TAP 70:30 SMF 9pm, 1310/1550nm,LC	0811F0621

Cordialmente,

STAR Inteligencia y Tecnología S.A.

OSCAR ALIRIO REYES
GERENTE GENERAL

Anexo 4

XXXXXXXXXXX

Bogotá D.C. 25 de Noviembre de 2010

Señores
BANCOLOMBIA
Ciudad

GG-OF-402

Por medio de la presente autorizo al señor John Jairo Castro Chica, identificado con Cédula de Ciudadanía No. 10.255.795 de Manizales, para recoger documentación de apertura de cuenta conjunta entre STAR Inteligencia & Tecnología S.A. y Fiscalía General de la Nación.

Gracias por su atención

Cordialmente

STAR Inteligencia & Tecnología S.A.

Oscar Alirio Reyes Castro
Representante Legal