IMPORTANTE! El siguiente Informe ha sido elaborado en base a un cuestionario con preguntas básicas, que le hemos enviado oportunamente a nuestros anunciantes. Si a usted, como lector, le interesa aportar alguna información adicional que enriquezca el tema, no dude en enviarnos sus comentarios a nuestra editorial a: editorial@rnds.com.ar Publicaremos los mismos en sucesivas ediciones.

Espionaje electrónico

Micrófonos y cámaras ocultas han dejado el terreno de la ficción para ser parte de la vida diaria.

Al espionaje electrónico se lo conoce con el nombre de medidas electrónicas y al contraespionaje como contramedidas electrónicas. En este informe analizaremos los equipos utilizados para ejercer dichas acciones y la última tecnología aplicada a los mismos.

Podría decirse que muchos de los actuales recursos de la vida moderna nacieron en la clandestinidad, guardados como grandes secretos de estado que, luego, por algún (desconocido) motivo dejaron de tener interés. O dejaron de ser útiles para fines militares. O los mismos creadores vieron que, además de útiles para el gobierno de un país, podían ser útiles y lucrativos para las grandes empresas de ese país. Difícil discernir.

En algún momento el radar fue secreto y hoy es una herramienta de uso civil y comercial importantísima. El *Kevlar* (fibra de carbono) fue también un secreto celosamente guardado mientras que en la actualidad pueden comprarse prendas confeccionadas en ese material en tiendas medianamente especializadas. Si hasta el GPS, el láser e Internet fueron secretos. Y por poseer estos grandes adelantos se entablaron guerras. Guerras silenciosas, protagonizadas por un ejército reducido, especializado, de recursos ilimitados. Soldados tras el más preciado de los bienes: información. Gente capaz de engañar y hasta matar por la clave de ese secreto. Los espías.

Definición

En términos de definición, "*espionaje*", la acción de "*espiar*" significa "*acechar, vigilar cautelosa o disimuladamente lo que alguien hace o dice*", lo cual implica, entonces, que el "*espía*" es el encargado de realizar esa acción.

La literatura, el cine y la televisión están plagados de espías, algunos portadores de elementos fantásticos para la época en que transcurren sus vidas y otros, capaces de realizar su tarea simplemente con lo que la naturaleza y tecnología de cada tiempo permitía.

Así, por ejemplo, una verdadera perlita es la técnica para enviar mensajes secretos en un huevo duro que ofrece *Bernard Newman* (1897-1968, autor de, entre otros, *La conspiración Gibraltar, El caso del espía de Berlín y Spy catchers*) en uno de sus relatos: "*Mézclese alumbre con vinagre hasta obtener la consistencia de la tinta y escríbase el mensaje en la cáscara. Cuando la tinta se seca, nada se ve, pero algunas horas más tarde el mensaje (que debe escribirse con letras grandes) aparecerá en la parte blanca del huevo*".

Lejos de esa auténtica artesanía del espionaje, comenzaron a verse -a partir de los años '50 y, especialmente durante la denominada Guerra Fría (período que se extendió desde el fin de la Segunda Guerra, 1945, hasta la desintegración de la Unión Soviética, 1991), caracterizada por el espionaje mutuo entre Estados Unidos y la URSS- elementos cada vez más sofisticados, de menor tamaño y mayores prestaciones. Así nació un emblema de la literatura fantástica: *James Bond, 007*, el agente británico con licencia para matar, capaz de sacar un arma de su anillo o convertir su corbata en una soga lo suficientemente larga como para escalar tres pisos.

La ciencia y la tecnología permiten hoy, sin llegar a tales extremos, la creación de elementos altamente sofistica-

Continúa en página 108

Viene de página 104

dos que, como decíamos al inicio, no sólo son aplicados en ámbitos militares sino también en el civil.

"*El espionaje existió, existe y existirá mientras se maneje información confidencial en cualquier parte del mundo*" explican desde **High Security La Casa del Espía**, una de las empresas especializadas en venta de equipos tecnológicos para ese fin. "*En la actualidad -amplían-, el avance tecnológico y las comunicaciones globalizadas permiten el libre acceso a la información para desempeñarse y capacitarse en el mundo del espionaje, muy diferente al pasado, que dicha información y capacitación eran exclusivamente de organismos oficiales*".

Qué pasa en Argentina

Como dijéramos, en un principio las tareas de inteligencia (o espionaje) eran exclusivas de las Fuerzas Militares. En nuestro país, por ejemplo, durante la presidencia de Juan Domingo Perón se creó un organismo de estado llamado Control de Gestión, que luego se transformaría en el *Servicio de Inteligencia del Estado* (SIDE). Este organismo estaba a destinado a realizar las tareas de inteligencia y contrainteligencia dentro de la República Argentina, aplicado básicamente al ámbito político.

¿Qué pasaba con el espionaje en las esferas civiles? "*El espionaje civil en Argentina comenzó en la década del '90 y, creo, fue uno de los primeros vicios que recibimos vinculados a la globalización*", explican desde **Spy Products**, otra de las importantes empresas proveedoras de elementos para el espía en Capital Federal.

Ahora bien, ese exceso de información y tecnología debe encontrar un ámbito adecuado para ser aplicada. De lo contrario, no tendría razón de existir. Y en nuestro país, los ámbitos en los que más se aplica es en el comercio y la industria.

"*Esto se vio mucho en la época de la recesión económica de nuestro país, cuando era mucho más barato robar una idea o producto que desarrollar la ingeniería necesaria para fabricarlo*", asegura uno de los especialistas consultados.

Por su parte, desde **High Security La Casa del Espía** aseguran que, si la pregunta hubiese sido formulada en los '90, la respuesta hubiese sido "*en el ámbito industrial*" pero actualmente "*la información estatal es tan vital como la industrial, porque cuando existen intereses políticos y de poder manejar información precisa puede ser clave en muchos organismos estatales*".

Aunque de otra índole, una buena prueba de que el espionaje en Argentina está vigente es la violación de correo electrónico sufrida por dos periodistas de Clarín, caso aún sin demasiadas explicaciones ni definiciones.

¿Legal o ilegal?

Es lógico pensar que se considere al espía como alguien que trabaja al margen de la ley ya que, históricamente, debían trabajar encubiertos, ocultando su verdadera labor y ocultándose de las autoridades. Cuando se trata de espionaje militar, incluso, la exposición pública podía significar la muerte.

"*La venta de elementos para espionaje en Argentina, hasta que no salga algún tipo de legislación o jurisprudencia que diga lo contrario y mientras el comercio page sus impuestos y esté al día con la AFIP, es totalmente libre, free*", explican de **Spy Products.**

"*Existe una ley contra quien atente la seguridad de la Nación Argentina, realizando acciones de espionaje y sabotaje: es la LEY 13.985. Pero no hay una ley que regule la venta de este tipo de equipos en Argentina y tampoco en otros países del mundo*", amplían desde **High Security La Casa del Espía.**

¿Para qué espiar?

Los fines que persigue un espía o quien manda a espiar son muy variados, aunque hay una tendencia: hoy, los sectores privados, antes de recurrir a una empresa de investigaciones prefieren adquirir algún tipo de dispositivo electrónico que posibilite la obtención de información.

Claro que no siempre los compradores de dispositivos para espías persiguen fines ilegales sino más bien lo contrario: protegerse de un posible espionaje o descubrir un espía en su empresa. Generalmente, estas personas se encuentran con problemas de empleados desleales, estafas o actos de corrupción dentro de sus propias empresas, por lo que desean averiguar ellos mismos quién es la persona que está entregando esa información a la competencia.

En estos casos, la utilización de dispositivos electrónicos es uno de los medios más eficientes y rápidos de detectar ese tipo de sabotaje.

Para contrarrestar el daño del espía existe el contraespionaje (en el idioma militar) o las contramedidas, en el más moderno de los lenguajes electrónicos.

Qué usar

Así como 007 era capaz de hacer aparecer un arma de su cigarrera y el inefable Maxwell Smart podía comunicarse con sus superiores a través del "*zapatófono*" (un teléfono incorporado en el zapato), los espías modernos cuentan con un variado número de aparatos para poder llevar a cabo su tarea: desde cámaras y micrófonos incorporadas a la ropa o elementos de uso cotidiano (lapiceras, relojes, anteojos y siguen las firmas...) hasta encriptadores e inhibidores de celulares.

Existe una ley contra quien atente la seguridad de la Nación Argentina, realizando acciones de espionaje y sabotaje: es la LEY 13.985. Pero no hay una ley que regule la venta de este tipo de equipos en Argentina y tampoco en otros países del mundo.

A continuación, un breve listado de los elementos más comunes y que pueden conseguirse (a no muy módicos precios, por cierto) en cualquier spyshop que se precie de tal.

Artículos para espionaje

Entre los más comunes se encuentran los micrófonos en sus distintas variantes (ocultos en las ropas, algún elemento de uso cotidiano o en algún lugar de una oficina o sala de reuniones), cámaras y microcámaras, transmisores GSM y encriptadores telefónicos.

- **Micrófonos inalámbricos:**

- Receptores y micrófonos: Son equipos de alta sensibilidad de recepción, con rangos de hasta 999 Mhz, lo cual

Continúa en página 112

Viene de página 108

permiten su adaptación a cualquier otro sistema de comunicaciones. Por su reducido tamaño pueden ser utilizados en operaciones de inteligencia. El monitoreo de estas unidades puede realizarse a través de parlantes (externos o incorporado) o en forma discreta conectándole auriculares. Desde la salida de audio, además, puede ser conectado a cualquier grabador analógico o digital.

- Antenas: Las antenas están diseñadas para poder recibir la señal de los micrófonos, cuya variedad más versátil es la antena para autos: colocada sobre el techo de un vehículo, la recepción del audio será más eficaz. Hay dos variedades: las que son preparadas para recibir únicamente dentro de la banda de los micrófonos -que darán un mayor rango de recepción- y las antenas diseñadas para una frecuencia determinada (antena dedicada).

- Micrófono ambiental: La sensibilidad, estabilidad y recepción de este tipo de micrófonos es notable. Suele ser utilizado para operaciones encubiertas exigentes por su facilidad de instalación: su reducido tamaño lo convierte en ideal para ser sembrado bajo las mesas, simplemente pegándolo con un sticker doble faz. Estos micrófonos, cuando no vienen ya incorporados a distintos elementos de la vida diaria, pueden ser fácilmente plantados en ellos. Entre los objetos más utilizados actualmente se encuentran: bolígrafos, calculadoras, mouses y parlantes de computadoras, celulares y hasta en las baterías de los celulares.

- Estetoscopio microfónico: Funciona bajo el mismo principio que el estetoscopio médico, pero suma un poderoso micrófono. Con estos equipos, el micrófono de contacto se apoya sobre una pared de un grosor de hasta 35 cm, logrando una recepción nítida de lo que sucede del otro lado de la pared sin correr el riesgo de ser detectado. Viene generalmente con un amplificador, que cuenta con una perilla de regulación de volumen, un swicht para conectar el micrófono cerámico que se apoya en la pared y dos salidas, una de auriculares y otra para conectar a un grabador.

- Transmisores GSM: Son la novedad y los "*chiches*" del mercado. Son dispositivos ideales para monitorear objetivos mientras la persona está fuera de su lugar habitual. El transmisor funciona con tecnología GSM, por lo que hay que insertarle una tarjeta SIM (preferentemente anónima). Luego se "*llama*" desde un teléfono especifico previamente seteado al número de la Sim y el transmisor contestará automáticamente sin producir ningún ruido que alerte su presencia. Estos dispositivos suelen tener entrada opcional para micrófono externo que se activa mediante un swich de selección.

• **Grabadoras compactas de audio y video:** Las hay de diferentes tipos: analógicas y digitales, de audio, video o audio y video. Las más modernas son las videograbadoras digitales, de muy reducido tamaño *(entran en el bolsillo de un saco)*. Las ventajas por sobre los anteriores es su tamaño, lo cual posibilita que cualquiera pueda portar un sistema de cámara oculta en el cuerpo, prácticamente sin darse cuenta. Vienen con una entrada para la señal de audio y video y la grabación queda almacenada en la memoria interna *(de hasta 20 Gb)*, logrando hasta 22 horas de grabación en alta calidad (28 cuadros/segundo). Algunos modelos tienen la opción de grabar en una memoria externa SD. La visualización de imágenes puede hacerse a través de la misma grabadora o conectándola a un televisor (por RCA) o una computadora (por USB).

• **Cámaras Ocultas:** Funcionan como cualquier cámara tradicional pero tienen la ventaja de ser perfectamente camuflables en distintos elementos y transmiten de manera inalámbrica. Un ejemplo: una cámara camuflada en un par de anteojos puede utilizarse para filmar en cualquier ambiente. La microcámara, por lo general, se coloca en el centro del armazón, lo que permite filmar exactamente lo que se está mirando y de la patilla sale un cable texturado de hilo igual a un sostenedor de anteojos, que puede ser conectarlo al transmisor de audio y video camuflado entre las ropas. El transmisor tiene una entrada de Audio y Video Plug y en su interior se encuentra un micrófono amplificado que captará las conversaciones de ese ambiente. Transmite la señal de largo alcance hacia un maletín receptor.

• **Maletín receptor:** El receptor de audio y video recibe la señal de la cámara inalámbrica. Posee dos salidas RCA, una de audio y una de video que con un cable se conecta al minigrabador, donde se puede monitorear la filmación a distancia y a la vez realizar la grabación en formato digital. Esta grabación puede ser reproducida en formato analógico desde una TV o en formato digital en una computadora, descargando el archivo con un cable USB. Estos equipos suelen incluir una antena omnidireccional para auto. El maletín ofrece dos opciones: poder realizar la recepción a distancia o bien portarlo uno mismo junto con el sistema de cámara inalámbrica.

• **Celular espía:** Son celulares GSM que, para activar el sistema se requiere de dos aparatos: un celular modificado y otro (de cualquier tecnología) que hará la llamada hacia el primero, activando el micrófono oculto en el interior. Para realizar la activación remota (sin límites de distancia), hay que llamar al número del "*celular espía*" desde el celular captor. Recibida la llamada, en el espía se activará el micrófono, que permite oír conversiones hasta a 10 metros de donde se encuentra el aparato. Este tipo de aparatos, además, operan como un celular común, permitiendo emitir y recibir llamadas con total normalidad salvo que se lo llame desde el celular captor. Ante esta llamada, responderá de manera automática abriendo el micrófono sin alertar al usuario ni a quienes lo rodean.

Los equipos de espionaje, llamados en inteligencia Medidas Electrónicas, son dispositivos o equipos con capacidad para captar información audible, visual o ambas para monitorearlas o grabarlas y enviarlas por un determinado canal, discretamente, hacia otro punto.

Contramedidas electrónicas

Los elementos disponibles para contrarrestar el espionaje también se enumeran en una larga lista. Los de uso más frecuente, en tanto, son los siguientes:

• **Detectores de radio frecuencia:** Son utilizados para detectar cámaras y micrófonos inalámbricos instalados en distintos sitios de una oficina, sala de

Continúa en página 116

Viene de página 112

reunión o habitación. Tienen una alta sensibilidad, cuyo rango de detección va desde 1 Mhz hasta 6 Ghz, ancho de banda donde se encuentran el 99,9 % de los dispositivos de transmisión encubierta, tanto de audio como de video. Algunos permiten la incorporación de un filtro de frecuencias de radio FM. Estos detectores son portables y pueden ser utilizados en reuniones, dentro del bolsillo interno del saco, para detectar en modo de vibración silenciosa la presencia de una determinada frecuencia dentro de ese ambiente. También son capaces de localizar dispositivos de transmisión vía GSM o TDMA.

• **Interceptor de video inalámbrico:** Pueden interceptar fácil y rápidamente señales de cámaras ocultas inalámbricas. Son receptores automáticos diseñados para realizar un barrido de frecuencias en el rango de los 900 hasta los 2520 Mhz, ancho en el que encuentran el 100% de los sistemas de filmación encubiertos utilizados en la actualidad. Al detectar una señal de video, automáticamente suena una alarma y en un display de alta resolución se puede ver la imagen color o blanco y negro. La distancia de recepción depende de la potencia utilizada en los transmisores de video.

• **Reflectómetro telefónico:** Trabaja con el mismo principio que opera un radar, enviando pulsos y esperando su reflejo "*retorno*" para procesar la información recibida. Una vez conectado sobre la línea telefónica envía un pulso eléctrico a lo largo de esa línea hasta el interior de la empresa proveedora. Cuando el pulso llega al final de la línea o encuentra un paralelo "*puente*" retorna a la unidad mostrando las diferencias de energía sobre su recorrido. Este instrumento verifica y localiza anomalías sobre el trayecto de la línea, identificando el sitio del "*puente*" o la anomalía en un rango menor a los 30 cm.

• **Analizador de espectro:** Es un sistema de contraespionaje controlado por microprocesador con un analizador de espectro incorporado diseñado a medida, que puede operar automáticamente, almacenando en la memoria todas las señales encontradas para una posterior revisión.

• **Perímetro anti-micrófonos:** Dispositivo diseñado para crear un perímetro seguro en un ambiente determinado (oficina, despacho o sala de juntas) que genera un ruido acústico interno que anula micrófonos alámbricos, inalámbricos o de contacto instalados sobre o dentro de las paredes, transmisores de audio ubicados en las tomas de corriente y también produce vibraciones en los vidrios de las ventanas impidiendo que los micrófonos láser de tecnología militar puedan demodular la señal de audio dentro de ese ambiente. El sistema "inyecta" el ruido dentro de las paredes, produce vibraciones en los vidrios y no en el ambiente, por lo que permite una conversación normal mientras rechaza y anula cualquier dispositivo espía.

• **Microdetector para celulares:** Es un dispositivo electrónico capaz de detectar radiofrecuencias riesgosas (de 5 Mhz a 2,5 Ghz) producidas por un celular. Esta unidad puede ser portable o apoyada en el escritorio, siempre cerca del celular. Así, cuando el celular emite una transmisión oculta de su conversación, en modo stand by (no debe estar transmitiendo datos) el micro detector adoptara la RF emitida por el celular y automáticamente empezará a vibrar en forma silenciosa. Puede detectar y alertarle desde las intervenciones más sencillas hasta las más sofisticadas desde un celular en modo de micrófono intruso.

• **Inhibidores celulares:** El sistema de inhibición celular fue desarrollado por tecnologías militares con el fin de anular las comunicaciones a su enemigo pero pasó a los organismos gubernamentales y actualmente su uso se extiende hasta el ámbito civil. Este sistema interfiere la señal entre el celular y la torre base con la cual se está comunicando emitiendo ondas de Radio Frecuencia en baja potencia, que alcanzan para bloquear comunicaciones celulares hasta 30 metros de radio condiciones óptimas. Al activarse, los celulares tardarán entre 1 y 20 segundos en perder la conexión con la torre y aparecerá en la pantalla "*Sin servicio*" o ésta permanecerá normal pero no podrá emitir ni recibir llamadas dentro del área de inhibición. Una activado el inhibidor, todas las llamadas entrantes ingresarán directamente al contestador como si el celular se encontrara en un área fuera de cobertura.

• **Encriptadores:** Existen dos tipos, pero ambos funcionan bajo el mismo principio: las dos puntas de la comunicación deben tener el encriptador correspondiente.

- Encriptadores celulares: Los últimos modelos utilizan tecnologías GSM o TDMA, no requieren de baterías, ya que se alimentan de la misma batería del celular y no necesitan ser "*llamados*" desde un número especifico. Para activar el modo seguro basta correr una perilla y comenzará la encriptación entre dos celulares. Siempre la encriptación debe ser entre dos celulares con el mismo módulo encriptador. Así, uno se comunica con el otro en forma independiente y uno solo envía la señal de codificación (algoritmo), que variará entre llamado y llamado en forma aleatoria.

- Encriptador telefónico fijo: Asegura las comunicaciones de voz prácticamente contra cualquier tipo de escuchas, hasta las realizadas por la compañías telefónicas. El módulo encriptador se conecta entre el microauricular y el teléfono y sólo hay que pulsar un botón para comenzar con la codificación. La encriptación únicamente puede realizarse punto a punto, por lo cual siempre los dos lados de la comunicación deben tener colocados estos encriptadores. También puede organizarse una red de más d e dos encriptadores, pero únicamente la encriptación se logrará entre dos puntos.

Las Contramedidas Electrónicas son acciones planificadas e implementadas con el objeto de proteger informaciones sensibles propias y neutralizar, detectar, localizar o perturbar las acciones de espionaje electrónico que se ejerzan sobre el objetivo.

Agradecemos para la elaboración de este informe la colaboración de:

Nicolas Ruggiero
(HIgh Security, La casa del espía)
www.lacasadelespia.com

Ernesto Yaffe
(Spy Products, Todo tecnología)
www.spyfull.com