4. ELECTRÓNICA

Una mirada desde las actividades de contramedidas de vigilancia técnica

(Technical Surveillance Counter Measures)

Por el Teniente Coronel (retirado) OIM Carlos Federico Amaya (*)

ABSTRACT

Poco se escribe y publica sobre este capítulo de la seguridad, que supone un largo y profundo conocimiento de tecnologías desde el punto de vista de la ciencia básica y nos obliga a reflexionar sobre las capacidades y concientización que debe desarrollar el líder de seguridad ante el ataque de la infiltración electrónica.

El presente artículo no pretende bajo ningún concepto sentar jurisprudencia sobre los procedimientos del buen arte en lo que respecta a lo específico de la seguridad técnica de la información y las telecomunicaciones.

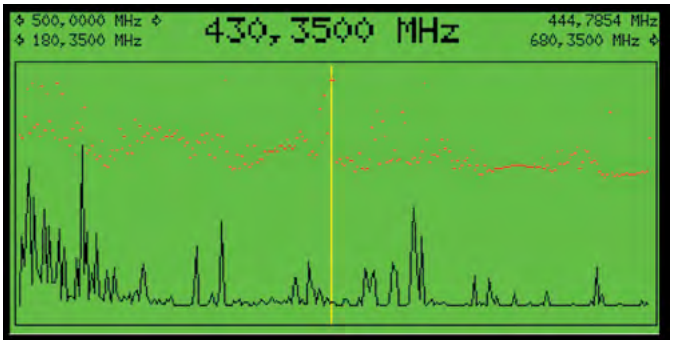
Solo busca volcar experiencias por mí recogidas a lo largo de algo más de 40 años de trabajo técnico en las áreas de la guerra electrónica, en lo específicamente referido a contramedidas de vigilancia técnica y su aplicación en las actividades cívico-comerciales.

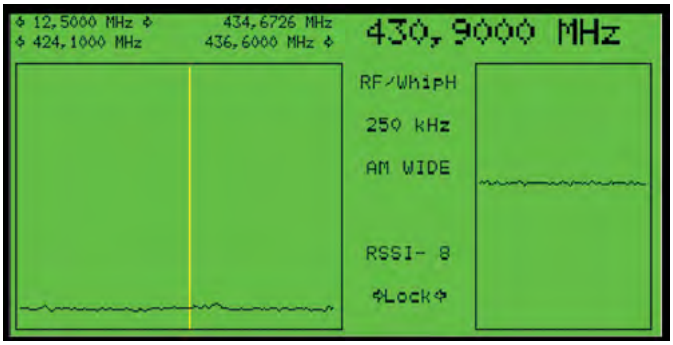
Trataré de desarrollar los temas en forma absolutamente coloquial y muy sintética, enfocando los conceptos técnicos hacia las actividades netamente gerenciales o de liderazgo de los equipos humanos que materializan la seguridad de empresas e instituciones, ello con el objeto de despertar inquietudes y sentar algunos principios que considero de utilidad para la gestión de mis colegas.

Lo expresado en el párrafo anterior no implica el hecho de que el líder del equipo de seguridad no deba tener en su preparación ciertos conceptos de ciencia básica, dado que el teatro de operaciones donde se desarrolla principalmente la actividad de telecomunicaciones es precisamente el espectro electromagnético.

Hago hincapié en ello dado que la evolución de la **ciencia aplicada** es tan rápida que hace prácticamente imposible para el líder vivir en la **“cresta de la ola”** de la tecnología como auxilio de su gestión. Pero la cosa cambia si entendemos el fenómeno físico conceptualmente, dado que el mismo no varía y, de esta manera, rápidamente podremos interpretar por dónde pasa la evolución dándonos cuenta de que **“lo que cambia y evoluciona son los ingenios y no la ingeniería”.**

Es de destacar que el propósito de los estudios de TSCM *(Technical Surveillance Counter Measures)* es localizar y neutralizar dispositivos de vigilancia electrónica instalados subrepticiamente con el objetivo de robar información. Para ello, es necesario, en primer término, identificar las características de la "firma electromagnética" del predio en análisis, de modo que la misma se constituya en un antecedente de análisis por comparación sobre el área en cuestión en futuros trabajos.





Entendemos por "firma electromagnética" en nuestro ámbito de trabajo al registro de las características de las emisiones radioeléctricas que predominan en el predio en estudio.

Esto se logra por medio del empleo de equipos que genéricamente se denominan "analizadores de espectro", muchos de los cuales se ofrecen en el mercado, adaptados al uso específico de las actividades que nos ocupan. Ellos detectarán en mayor o menor grado las emisiones producto de la activación de transmisores (emisores de radiofrecuencia) desde frecuencias del orden de los pocos megahertz hasta algunas decenas de gigahertz.

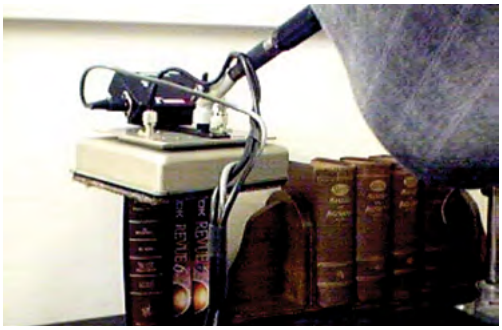
De esta manera, se detectarán en mayor o menor grado, todos aquellos ingenios que hayan sido "sembrados" en forma clandestina y estén activados.

Dentro de las leyes físicas que describen el fenómeno de radiación electromagnética, es importante destacar que el parámetro físico que varía es la densidad del ambiente en el cual la perturbación se propaga y es por ello que aunque la perturbación electromagnética se desplace por el aire, el agua

(incluyendo la humedad y el rocío) o los sólidos (metales y desde los años 60, la fibra de vidrio que da el puntapié inicial al uso masivo de la fibra óptica), podemos ver que las leyes que describen su comportamiento son las mismas.

La pregunta es ahora ¿con qué instrumento contamos para ayudarnos a detectar ingenios electrónicos que no emiten electromagnéticamente?

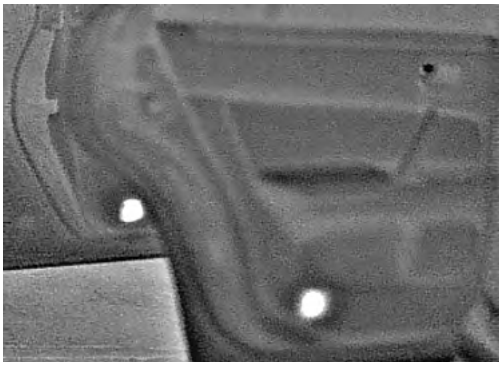
La contestación es múltiple y partiremos nombrando y describiendo brevemente los que por experiencia personal más he usado y ellos son, en primera instancia, los medidores de junturas no lineales, que basan su funcionamiento sobre el hecho de provocar una emisión electromagnética como producto de la diferencia de potencial inducida entre los elementos electroquímicos y bimetales que conforman los componentes electrónicos de los circuitos. El fenómeno descripto se materializa al someter los componentes al "bombardeo" de un campo electromagnético que el mismo analizador de junturas produce.

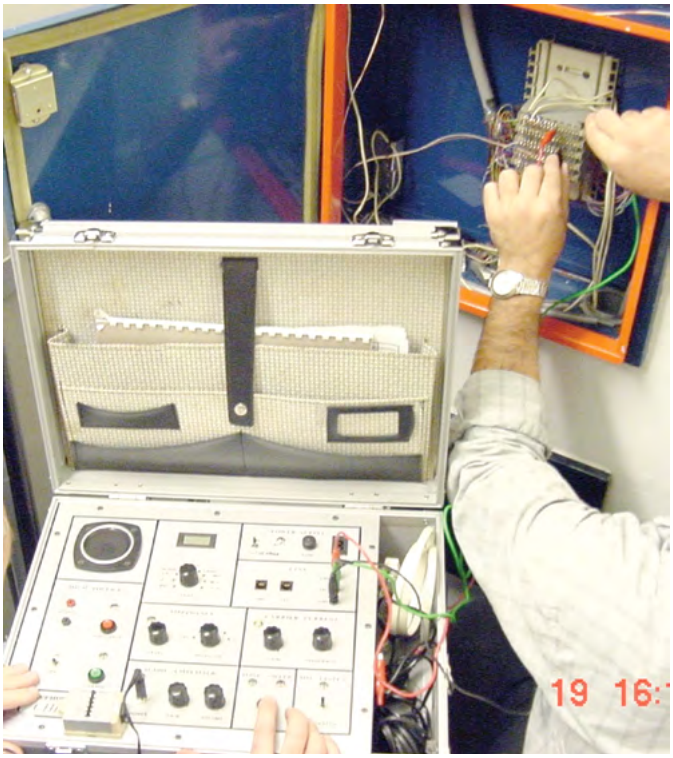


La tercera gran ayuda con que contamos para la detección la brindan equipos que trabajan bajo las características de la región de la optoelectrónica. Allí consideramos la imagen térmica y en cierto modo también la amplificación de luz residual.

Para el caso de las cada vez más difundidas cámaras de imagen térmicas, tan usadas para actividades de seguridad. En las actividades de TSCM, su uso es especialmente como detección de la energía electromagnética disipada en forma de calor, producto en la mayoría de los casos de desadaptaciones de impedancias en el diseño de los ingenios subrepticios. Debemos tener en cuenta que los objetos que buscamos para neutralizar, juegan con el inconveniente de superar la dificultad de diseño que implica su miniaturización.

Por último, las líneas telefónicas, las de transporte de energía eléctrica, de audio etc. Para la detección de conexiones clandestinas necesitan del empleo de distintas variedades e ingenios de equipo "ecómetros" y analizadores de líneas, basando su uso en principios de RADAR para localizar la





infiltración los primeros y la medición de parámetros técnicos (impedancias características, diferencias de potenciales, modulaciones, transmitancia, capacitancia etc.), los segundos.

Estas son, a mi criterio, las tecnologías básicas con que todo equipo de TSCM debería contar.

Pero atención, **"nada reemplaza al hombre, su experiencia y entrenamiento".** De nada vale tener equipamiento si para cada una de las tecnologías no tenemos el hombre especializado en el equipo.

La experiencia me indica que la mayor cantidad de casos de éxito en la búsqueda y detección han sido materializados por la experiencia y entrenamiento del hombre que "sabía mirar" y conocía sobre el estado del arte de lo que se usaba en cada época, en cada caso y en cada lugar del mundo. Esto solo se consigue con un profundo y serio entrenamiento respaldado por igual sentido de responsabilidad, profesionalismo y lealtad.

El hombre que realiza este tipo de actividades sabe mucho de su protegido, conoce hasta los últimos rincones donde él desarrolla sus actividades, en muchos casos conoce el lugar donde se mueve con su familia y es por ello que el potencial humano en esta actividad de TSCM es el principal factor a considerar y cuidar.

Es recomendable realizar estos estudios en forma asistemática y dentro de un adecuado programa de análisis de riesgo y salvaguarda de la información, en especial sobre aquellas áreas que comprendan los lugares de trabajos de ejecutivos, grupos de toma de resoluciones estratégicas o donde se procese información de valor.

Antes de iniciar una actividad de TSCM, al igual que cualquier actividad de gerenciamiento de seguridad, es necesaria la realización de un análisis de riesgo.

Entendemos por **análisis de riesgo** a la gestión que realizamos tendiente a:

> Establecer el contexto donde los riesgos se desarrollan.
> Evaluarlos.
> Consultar y tratarlos con la organización.
> Por último, monitoreo y revisación que a su vez lo realimenta.

Las tareas deben ser ejecutadas por una estructura capaz de soportar todos los procesos sin intervenir en ellos y en función de los objetivos de la seguridad y de aquellos estratégicos de la organización.

Es recomendable proponernos, gestionar los riesgos repensando la seguridad como integrada a la empresa, uniendo todos los programas bajo una única gestión.

Los trabajos de TSCM, terminan con la presentación de un detallado informe escrito de lo analizado con propuestas, observaciones y análisis de procedimientos, hábitos y emisiones radioeléctricas internas o externas en "tiempo real".

Es conveniente, con el auxilio de los responsables del mantenimiento y programación, auditar la configuración lógica del conmutador (PABX) en caso de existir o del servidor local para el caso que se cuente con telefonía IP, ello con el fin de determinar la situación de riesgo de los siguientes parámetros:

> Niveles de accesibilidad al sistema.
> Normativas de control de visitas de mantenimiento.
> Auditoría periódica de los internos.
> Procedimientos de verificación que eviten reprogramaciones encubiertas que permita:
    1. Llamadas sin costo.
    2. Correo de voz.
    3. Monitoreo de extensiones ocupadas.
    4. Creación de puentes a otras extensiones.

Por último, para acceder a la información necesaria para la planificación del servicio, así como para el desarrollo de este, el contratado debe ofrecer la firma de un Acuerdo de Confidencialidad para las informaciones a las que tenga acceso por la realización de los trabajos.

Este breve artículo, como expresara al comienzo, constituye solo un planteo general de experiencias recogidas del trabajo cotidiano de TSCM en el marco mundial, no se ha entrado a analizar el ataque informático o el ciberdelito, temas estos de los cuales mucho se habla y hablará.

He expuesto temas cotidianos de los cuales cada uno de ellos supone un largo y profundo desarrollo en futuras publicaciones, dejando como reflexión final el valor de la actividad de concientización que debe ejercitar el líder responsable de la seguridad de contra infiltración.

(*) Teniente coronel (retirado) OIM Carlos Federico Amaya: Oficial retirado del arma de Comunicaciones del Ejército Argentino, egresado del Colegio Militar de la Nación, es Ingeniero Militar de la especialidad Electrónica, recibido en la Escuela Superior Técnica del Ejército "General de División Manuel Nicolás Savio"; Perfeccionó su especialización en Institutos de Investigaciones científico-técnica de su país (CITEDEF) y en la Ecole National Superieure de Techniques Avancees (ENSTA-París).

Es Diplomado en Alta Dirección de Seguridad en Empresas (DSE) por el Instituto de Posgrado y Formación Continua de la Universidad Pontificia Comillas de Madrid, entidad en la que además se desempeña desde 2002 como Profesor Invitado de las materias "Protección de la Información", "Contra Medidas de Seguridad Técnica (TSCM)" y "Seguridad en Telecomunicaciones" en el Programa que esta Alta Casa de Estudios imparte en América Latina.

Se desempeñó como Jefe y Gerente de Seguridad en las Telecomunicaciones e Información de Telefónica de Argentina Sociedad Anónima, con responsabilidad sobre todas las actividades de contramedidas de seguridad técnica y seguridad de la información.

>>

Fue docente de la UADE, de la UCA Salta, asesor del Estado Mayor Conjunto en ciberdefensa, desde 2017 y hasta la actualidad es Subdirector de la Maestría en Ciberdefensa y Ciberseguridad de la Universidad de Buenos Aires en convenio con la Escuela Nacional de Inteligencia.

Es Investigador *Senior* en el Observatorio Argentino del Ciberespacio en la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas y miembro del Centro de Estudios de Prospectiva Tecnológica Militar "Gral. Enrique Mosconi" – Antena Territorial de Defensa y Seguridad de la Facultad de Ingeniería del Ejército.