"Redes Stay-Behind y el proyecto HARPOON"

David Marugán
@RadioHacking
www.davidmarugan.es
Octubre 2017

Este artículo forma parte de la introducción de la novela corta en la que estoy trabajando, así como del contenido de próximas charlas, que tratarán, entre otras cosas, de la formación e historia de las redes clandestinas de radio al servicio de ciertas organizaciones; fundamentalmente enfocado a la divulgación de las técnicas y equipos de radio clandestinos desplegados en diferentes contextos históricos. No se trata de un artículo profundo, sino como se ha dicho de introducción en el concepto de las Redes Stay-Behind y sus equipos, un tema sobre el que no hay mucho escrito en español.

Antes de adentrarnos en el contenido del artículo, me gustaría **agradecer muy especialmente su ayuda a Paul Reuvers y el equipo de www.cryptomuseum.com** , que me ha autorizado a poder usar su valiosa información y material fotográfico para documentar mis futuras charlas y avanzar en la novela corta. Sin este tipo de iniciativas de divulgación desinteresada y personas apasionadas por la tecnología sería muy complicado, por no decir imposible, poder investigar en estas áreas, donde en muchos casos el tiempo y la propia naturaleza reservada y secreta de la materia a tratar, hacen que sea muy complicado obtener datos técnicos fidelignos con los que empezar a trabajar.

¿Qué es una red "Stay-Behind"?

De forma muy sencilla y resumida se trata de una red secreta que está lista para actuar en caso de la invasión de un territorio por parte de un país enemigo. Los agentes operativos de esta red, desde el territorio ocupado y obviamente en la más absoluta clandestinidad, serían capaces de ejecutar operaciones de todo tipo a modo de resistencia encubierta. Pudiendo, entre otras muchas cosas, realizar:

- Sabotajes.
- Operaciones de desinformación.
- PSYOPS.
- Acciones violentas y de provocación.
- Atentados selectivos.
- Labores de inteligencia y espionaje.
- Establecer enlaces entre agentes y gobiernos en el exilio.
- Despliegue y mantenimiento de redes de radiocomunicaciones locales e internacionales.
- Etc.

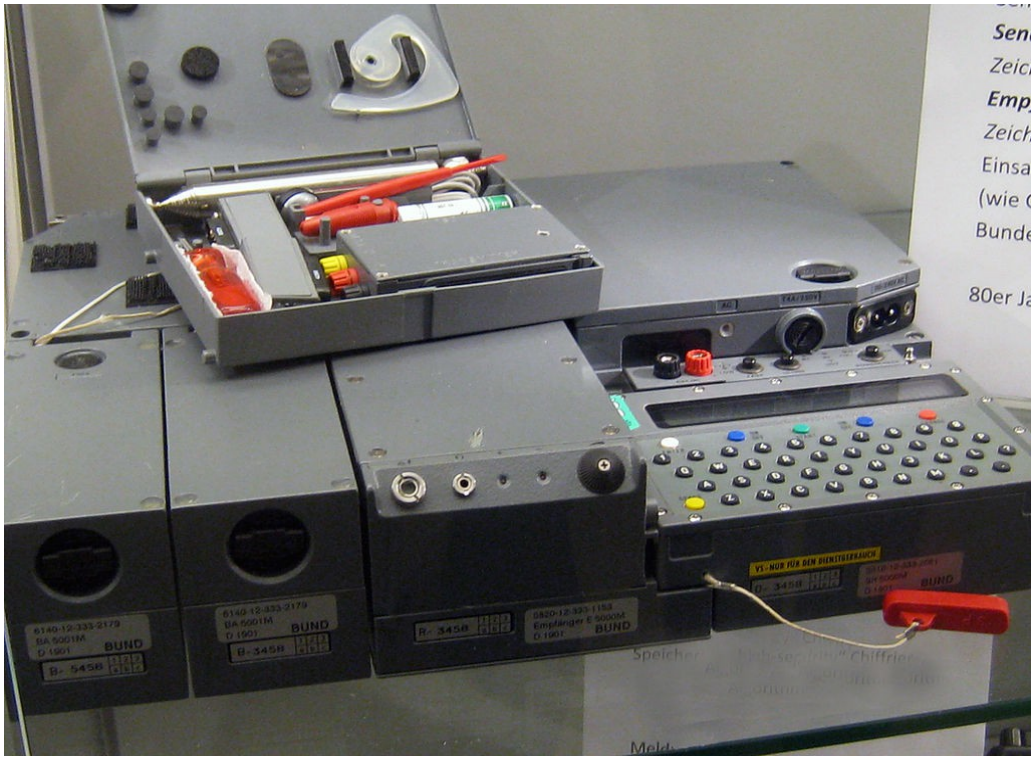
Las Redes Stay-Behind (a partir de ahora por comodidad RSB) tuvieron su momento de inicial de expansión durante la Segunda Guerra Mundial en los 50 y los movimientos de resistencia asociados al conflicto bélico, pero quizás la RSB más conocida por el público en general sea la relacionada con la denomidada Operación "Gladio"[1] ("Espada" en español) supuestamente puesta en marcha en Europa por la OTAN, en este caso, y aunque su nombre se asocia por el público en general a cualquier RSB, se trataría solo de la red desplegada en Italia (las RSB fueron implantadas en casi todos los países europeos aliados) y cuya existencia fue en parte reconocida por el Primer Ministro italiano Giulio Andreotti en 1990.

La polémica sobre este tipo de organizaciones es patente en la gran cantidad de libros y

1 https://en.wikipedia.org/wiki/Operation_Gladio

documentales publicados en tiempos recientes, siendo asociadas en muchos casos estas redes a actividades clandestinas e incluso graves atentados perpetrados en suelo europeo en tiempos de paz (lo que suele denominarse "terrorismo negro", entre los años 60 y 80, muy alejados de su actividad inicial de resistencia ante la ocupación enemiga. Este artículo tiene únicamente un fin de divulgación técnica de sus radiocomunicaciones, para profundizar en otras temáticas hay multitud de información en Internet, por lo que recomiendo a las personas interesadas buscar allí.

El Proyecto "HARPOON"



Estación SY-5000 completa. Imagen original: https://www.wikiwand.com/de/SY-5000

Durante la Guerra Fría, como es obvio, las RSB jugaron un papel fundamental ante una invasión por parte de la Unión Soviética. Uno de los problemas principales del establecimiento de las redes de radiocomunicaciones en las RSB desde la Segunda Guerra Mundial, fue la falta de homogeneidad en los procedimientos, cifrados y equipos usados en cada una de ellas. Otra cuestión muy importante, es que los operadores de aquellos equipos necesitaban una amplia formación en Código Morse, diseño de antenas, manejo de equipos, electrónica, etc. Tanto es así que en muchos casos el perfil adecuado, en caso de una red clandestina cívil por ejemplo, estaba limitado al de un radioaficionado experimentado, rumoreándose incluso la existencia en la Unión Soviética de una especie de "lista negra" de expertos en radio de países extranjeros que deberían ser "eliminados" en caso de invasión[2]. En cualquier caso, sea cierto o no, el hecho de tener "perfilados" a los operadores de los equipos es un evidente riesgo OPSEC y una gran limitación para estas redes.

Teniendo en cuenta que en cierto momento cada páis contaba con una RSB propia es lógico pensar que una de las prioridades fuera unificar ciertos criterios, como los equipos de radio, inviertiendo en I+D para desarrollar equipos que pudieran ser más fáciles de usar por cualquier agente con un mínimo de formación prévia, lo que como es logíco facilitaría el reclutamiento de agentes, dificultaría su perfilado, y por tanto mejorarían sustancialmente la operación y mantenimiento de estas redes clandestinas con ciertas garantías. También se debía tener muy en cuenta la importancia de su modularidad, protección ambiental y tamaño, sabiendo que los equipos

2 http://cryptomuseum.com/spy/gladio/index.htm

tendrían que ser escondidos y operados en ubicaciones secretas y desplegados en circunstancias muy complicadas. Por todo ello se decide a finales de los 70 desarrollar un sistema europeo de de comunicaciones unificadas, poniendo especial énfasis en la facilidad de uso de los equipos, integración de cifrado seguro compatible entre las distintas RSB y la posibilidad de incorporar un transmisor digital desatendido de banda estrecha, que pudiera transmitir los mensajes de forma segura incluso sin la presencia de un operador físico.

El nombre en código "HARPOON" se usó para denominar el proyecto secreto que se le encargó a Telefunken AEG en la segunda mitad de los 80 para desarrollar una estación de radio de HF con especificaciones militares denominada en algunos países europeos FS-5000, capaz de transmitir la información de las RSB a miles de kilómetros. Se trata de una estación modular, que una vez ensamblada puede realizar radiocomunicaciones criptográficamente seguras a larga distancia, y donde algunos de sus módulos pueden también ser operados de forma independiente, como por ejemplo la unidad de recepción o E5000 (en algunas versiones con ciertas modificaciones). Esto permitía cierta flexibilidad a la hora de realizar las diferentes configuraciones. El sistema completo, es denominado SY-5000. De forma resumida, los módulos de los que constaba la estación completa serían:

- Receptor de HF E5000, que además puede operarse en modo Stand-Alone.
- Transmisor con acoplador automático que permitía su operación sin grandes conocimientos técnicos usando un sencillo hilo largo como antena para todas las bandas. El transmisor que podía usar modulaciones muy sofisticadas como Vestigial Side Band Modulation o VSB, además de transmitir mensajes a "burst" o ráfagas ultrarápidas, que hacía prácticamente imposible su interceptación y posterior triangulación. Contaba con una potencia máxima de 25W 30W PEP y un rango aproximado de 2 MHz a 30 MHz
- Unidad de alimentación (PSU) y baterías.
- Digital Storage Unit (DSU), el controlador, que era considerada como la parte más importante del sistema, que además contenía el motor criptográfico y el RTC.
- Caja de herramientas básicas, que incluía por ejemplo una antena telescópica para la operación del receptor.
- Accesorios como cargadores, baterías, conectores, etc. Todos de alta calidad y estándares militares.

La unidad también cuenta en todos sus elementos y embalajes con protección contra el agua, conectores herméticos, etc. No entraremos en más detalles técnicos de la estación, porque se podría escribir un libro sobre el tema y porque una despcrición profunda y detallada del hardware, modulaciones y métodos criptográficos empleados puede ser consultada en:

http://cryptomuseum.com/spy/fs5000/index.htm

La lectura de este interesante y serio trabajo de Cryptomusem nos puede dar una idea de la importancia que tuvieron este tipo de equipos en aquella época. Además podremos ver esquemas técnicos y fotos de los equipos. Se trataría por tanto de un equipo puntero pensando en la época que se desarrolló y que todavía hoy tiene un gran interés de estudio.

El ocaso de "HARPOON" y objeto de "culto" para coleccionistas.

Poco antes de caer el Muro de Berlín estas unidades estaban dispuestas para la operación en las RSB, pero el devenir de la historia hizo que estos equipos fueran reutilizados en cierta forma por los Servicios de Inteligencia de algunos países hasta ser reemplazadas por otros equipos o usados en combinación con estos, como por ejemplo el equipo HF-7000 de Telefunken Racoms. Debemos tener en mente que estos equipos están diseñados de forma muy específica para las RSB y su operación clandestina, por lo que no resulta fácil darles un uso en la parte táctica militar, tarea para la que están diseñados otro tipo de equipos, si bien es cierto que muchos équipos dedicados a las RSB a lo largo de la historia han sido usados en comunicaciones secretas de carácter diplomático o relacionadas por los Servicios de Inteligencia.

El fin de la Guerra Fría y los escándalos que provocó el conocimiento público de las RSB y en particular el que se destapó en Italia con el nombre de "Operación Gladio", hizo que las redes clandestinas fueran desmanteladas a partir de entonces. Incluso en España el entonces ministro de Defensa Narcís Serra tuvo que ordenar una investigación sobre la presencia de estas RSB en el país[3].

Según parece, sobre el año 2000 un número reducido de unidades del FS-5000 sin material criptográfico, se filtraron "accidentalmente" y comenzaron a ser vendidas sin control gubernamental a través de los denominados Surplus o tiendas especializadas en electrónica militar. Hoy todavía pueden comprarse algunos equipos en estos mercados de forma legal y en algunos casos previa licencia para la importación de material de tipo militar (algunos países tendrían prohibido la exportación e importación de este tipo de materiales), aunque su precio y escasez son una dificultad añadida, sobre todo cuando se trata de un equipo completo y no una parte del mismo. Por tanto estamos hoy ante un preciado objeto de coleccionista, que en su día fue uno de los equipos más avanzados en comunicaciones secretas, usados en su día incluso por parte de la NSA en EE.UU o el BND alemán y que algunos radioaficionados han tenido la suerte de poder adquirir, modificar e incluso usar en sus comunicaciones radio en tiempos recientes. Incluso se pueden ver algunos videos en Youtube donde los propietarios operan las estaciones, algunos ejemplos:

- Demo de operación Stand-Alone de la unidad receptora FS-5000:
https://www.youtube.com/watch?v=CwbehXO6dPY
- Desembalaje y ensamblado del equipo:
https://www.youtube.com/watch?v=SclDz5AfUy8

Como suele ser ya costumbre en mis árticulos, no soy muy partidario de realizar conclusiones y únicamente me gustaría concluir invitando al lector interesado en comunicaciones encubiertas y radio en general, a formularse ciertas preguntas de interés:

¿Existen todavía hoy día estas redes Stay-Behind? ¿qué proposito tendrían en pleno siglo XXI? ¿qué tipo de equipos usarían? ¿es un modelo de red que puede ser exportado a otro tipo de organizaciones clandestinas o incluso de tipo criminal, fuera del ámbito puramente militar? ¿seríamos capaces de detectar su presencia?

Durante 2018 espero, si mis obligaciones profesionales y personales me lo permiten, poder terminal mi novela corta, dar alguna charla técnica sobre los equipos RSB y, si finalmente me es posible conseguirlo, mostrar algún equipo real de RSB o parte del mismo para ilustrarla y conocer más de su funcionamiento. Animo a todos los interesados en el tema a profundizar en este apasionante mundo de las radiocomunicaciones clandestinas y sus equipos.
73's.

3 https://elpais.com/diario/1990/11/16/espana/658710017_850215.html