



Secretos en el aire. La criptografía en la guerra civil española.

José Ramón Soler Fuensanta

Introducción.

Hace unos años escribí una pequeña introducción al tema de la criptología en la guerra civil española. La verdad es que me apetecía hacerlo; no existía prácticamente nada dedicado a tan curioso, y delicado a la vez, tema. El artículo se publicó en la web sobre la guerra civil en el país vasco de Alberto Bru, Jordi Pedrosa y Txema Prada (http://es.geocities.com/gce_euzkadi/paginas/cifra.html) y poco a poco fueron apareciendo enlaces a ese artículo, cosa que me llenó de satisfacción y de un cierto orgullo, inevitable cuando ves que un texto, aunque escrito como un simple divertimento, interesa a tanta gente. Recientemente, se me dio la posibilidad de ampliarlo en la presente web, cosa que agradecí inmensamente, y fruto de ello es este pequeño artículo que espero no desmerezca del anterior.

La criptografía y la guerra.

Decía Cicerón que *“cualquier género de paz entre los ciudadanos me parecería preferible a una guerra civil”*, sin embargo, a pesar de los siglos transcurridos, no se ha sabido sacar provecho de tan atinadas palabras. Nuestra patria fue testigo de una guerra civil larga, cruel, y posiblemente sin sentido, ya que no tiene sentido ni justificación una contienda en la que se lucha hermano contra hermano. No vamos a incidir en las causas de la guerra, ni políticas ni sociales, tan solo nos fijaremos en un asunto que solo en los últimos tiempos ha sido estudiado, la criptología, entendida desde sus dos vertientes, la criptografía o uso de sistemas para ocultar el contenido de un mensaje al enemigo y el criptoanálisis o métodos para poder descifrar esos mensajes sin ser el destinatario. El personal dedicado a ambas disciplinas pertenece, en general, a los servicios técnicos de los servicios de información militar, y, en el caso del criptoanálisis, junto con los datos obtenidos por radio escucha y observación permite obtener información sobre las intenciones del enemigo, su estado, y sus posibilidades de reacción.

A pesar de la afirmación de Groucho Marx de que Inteligencia Militar eran dos términos contradictorios, lo cierto es que la efectividad y el uso correcto de las fuerzas militares dependen en muchos casos de la inteligencia obtenida sobre el enemigo. Sun Tzu ya lo afirmaba hace siglos, y en la historia se ha demostrado que es cierto, siendo quizás más evidente en las guerras actuales.

El uso de la radio en los conflictos bélicos hizo que se estudiase su uso, sus limitaciones, y sus inconvenientes, el más evidente de ellos sin duda el hecho de que una onda puede ser recibida no solo por el destinatario de ésta, sino también por el enemigo. Nacen inmediatamente los servicios de escucha que se dedican a captar los mensajes enemigos y a estudiar toda la información que éstos aportan, no solo el contenido del mensaje, sino emisor, receptor,

frecuencia de los mensajes, ubicación del emisor y de los destinatarios de los mensajes. La información obtenida de esta manera, conjuntada con un buen sistema de archivo, permite obtener por inferencia mucha información. Paralelamente nacen o empiezan a aplicarse contramedidas contra tales escuchas, una de éstas es el uso de sistemas criptográficos para ocultar el contenido de los mensajes, y, evidentemente, hacen su aparición también los descryptadores, personajes encargados de romper los códigos y cifras enemigos y descubrir el contenido oculto de los mensajes cifrados con ellos.

La criptografía en la guerra civil.

Es unánimemente aceptado el hecho de que los sistemas de cifra utilizados por ambos bandos al inicio de la guerra eran muy sencillos. Esto hacía que su utilidad fuese muy baja ya que solo conseguían retrasar, en algunos casos solo unos minutos, la obtención del texto en claro por parte del enemigo. De todas maneras es justo reconocer que si hubo un bando que supo ver la importancia de ponerse rápidamente al día en estos asuntos, aconsejado sin duda por sus aliados alemanes e italianos, fue sin duda el nacionalista. En noviembre de 1936 adquieren diez máquinas Enigma alemanas para proteger sus comunicaciones diplomáticas (1). Ante la evidencia de que los diplomáticos preferían métodos más clásicos para cifrar, libros de códigos con supercifrado, y consideraban excesivamente complicadas dichas máquinas, éstas fueron distribuidas posteriormente entre los diferentes Estados Mayores de las diferentes zonas militares para proteger sus comunicaciones y para comunicarse con sus aliados alemanes e italianos. Durante la guerra fueron adquiridas varias más, así como otras máquinas de cifra menos seguras, como la Kryha (2). Sin embargo, a niveles inferiores se siguieron utilizando métodos menos sofisticados como tablas de homófonos y sistemas de cinta (3).

El bando republicano basó la seguridad de sus comunicaciones en un amplio abanico de métodos, aunque sin duda los preponderantes fueron los sistemas de cinta, los libros de códigos y los códigos de trinchera, éstos dos últimos generalmente supercifrados. Sin embargo vemos también que se utilizan sistemas, un poco modificados, como el playfair, utilizado por los guerrilleros, y sistemas de cinta múltiple con un pequeño repertorio, utilizado generalmente por la aviación. No tenemos constancia de la utilización de ninguna máquina de cifra por parte republicana, aunque sabemos que el ministerio de estado estuvo interesado en su adquisición.

Los servicios de escucha y descryptado.

Debemos ser francos y reconocer que conocemos mucho mejor la estructura de los servicios nacionalistas que la de sus homónimos republicanos. Los primeros tuvieron el acierto de unificar todos los servicios de criptografía, escucha y descryptado bajo la dirección de Antonio Sarmiento León-Troyano. Sarmiento logró montar una estructura centralizada en la que primaba la coordinación de los diversos grupos de descryptado (Palma de Mallorca, Zaragoza, Imker, Ufficio D, SIM, SIFNE, etc.) apoyándose en la excelente labor de personas como José María Iñiguez, Baltasar Nicolau Bordoy o Juan Solabre Lazcano, por citar solo a los más representativos. Los grupos de descryptado se coordinaban el trabajo y una vez descubierta una clave, ésta se repartía al resto de grupos para evitar duplicidades en el trabajo. La falta de ese repositorio central de claves, junto con una mayor coordinación de los servicios de escucha y descryptado, fue uno de los grandes errores del bando republicano. El servicio de descryptado del Estado Mayor de la República, que inicialmente fue asesorado y ayudado por personal soviético, estaba formado por personal muy competente (4), pero adolecía de falta de personal, medios y de una organización centralizada. Si bien en los últimos meses de la guerra se habían empezado a dar pasos en vista a una posible reorganización de los servicios, ya era demasiado tarde.

También sabemos de la existencia de un gabinete de criptografía del SIM; dicho gabinete debió formarse a finales del 38 o principios del 39. Hasta ese momento, los descryptados requeridos por el SIM eran realizados por el servicio de descryptado del Estado Mayor.

Algunos ejemplos.

La información obtenida por descriptado era ocultada en los informes nacionalistas detrás de un aséptico “de fuente segura”. La información obtenida por esta vía sirvió para que el crucero Canarias capturase, en la mañana del 8 de marzo de 1937, al buque “Mar Cantábrico” (5) cargado de armas con destino a la República. No es el único caso, los especialistas del Spets-Odel, el servicio de criptología soviético, consiguieron descriptar un mensaje nacionalista en el que se indicaba que de Marsella iba a partir un barco con destino a un puerto de la República con ciertas características externas. En el mensaje se informaba a un crucero y a la aviación para que hundiese el barco independientemente de la bandera bajo la que viajase. Esa información fue mandada a Marsella, donde estaba atracado el barco, evitando que se perdiese no solo el buque, sino varios especialistas soviéticos y personal de las Brigadas Internacionales (6).

Sin embargo no hay que pensar exclusivamente en términos inmediatamente militares, cualquier tipo de información obtenida era importante, moral en la población y en los soldados, aspectos económicos e incluso información sobre los ataques producidos. Verdaderamente importante era la obtenida de los descriptados que informaban sobre los bombardeos realizados, dado que, en muchos casos daban la información real de los daños producidos, o complementaban la que en los partes oficiales era generalmente camuflada u omitida. Centrándonos en Castellón, el 26 de abril el Gobernador Civil informaba al Ministro Gobernación de que (7):

“Ayer aviación enemiga a las nueve bombardeó Castellón en su aeropuerto y faro lanzando más de cien bombas sin causar daños. A las catorce volvió a bombardear y ametrallar intensamente población civil destruyendo treinta casas causando desperfectos en cien y matando cinco personas. Corte luz eléctrica. Almazora causó desperfectos hospital civil. Villareal derribó catorce casas cortando comunicaciones. Hubo seis muertos y veinte heridos. Moral del pueblo muy buena se trabaja intensamente para reparar todo desde primeros momentos. Vías comunicaciones quedarán hoy reparadas así como luz eléctrica. Salúdole.”

El 4 de mayo la aviación nacionalista bombardea otra vez Castellón. En el parte oficial de guerra republicano del día siguiente se dice que *“20 aparatos lanzaron más de 120 bombas destruyendo totalmente 60 edificios. A las 17 horas, 40 aviones arrojaron cerca de 300 proyectiles de gran tamaño que ocasionaron el derrumbamiento de 40 casas”*. Al día siguiente el Gobernador Civil envía un mensaje al Ministro de Gobernación informando del ataque de la aviación enemiga y de las precarias situaciones con las que debe hacer frente a estos ataques:

“Ayer aviación enemiga con 50 aparatos bombardeó intensamente dos veces Castellón, Cabanés y Almazora. Hubo 8 muertos 20 heridos porque hay buenos refugios. En Castellón destruyó más de 40 casas. En Cabanés de 30 a 40. Se plantea problema viviendas, que voy resolviendo. Necesitamos más refugios. Falta dinero. Ruego subvención. Ruego también gestionen algún antiaéreo. Salúdole.”

El 20 de mayo vuelve a repetirse el ataque, el parte oficial de guerra habla de que *“el ataque lo realizaron 19 aparatos “Junker” que lanzaron 190 bombas ocasionando la destrucción de sesenta casa, entre ellas el Hospital Militar, en el que cayeron ocho explosivos. El bombardeo causó víctimas entre la población civil.”*

Sin embargo, el informe que envía el día siguiente el Subdirector General de Seguridad al Director General es diferente:

“Participo a V.E. que a las 11 horas ayer fue bombardeado por aviación facciosa casco urbano Castellón causando daños consideración escasas víctimas. A las 16’45 horas hoy aviación facciosa bombardeó muelle esta capital causando daños buque guerra Almirante Lobo al que produjo vía agua, trabajando bomberos y marineros en reparación, también alcanzó petrolero

Campomanes incendiando parte izquierda que fue sofocado rápidamente siendo escasos los daños. No hubo víctimas. Resto territorio sin novedad. Salúdle.”

El 9 de junio el puerto de Castellón es bombardeado, si bien no aparece información alguna del hecho en el parte republicano de ese día, los miembros del gabinete de descryptado del V C. de E. captaban y descifraban el día siguiente un mensaje de Barcelona a Valencia en el que se informaba que el puerto de Castellón había sido bombardeado y que habían caído varias bombas sobre el “Isadora”, pero que las bombas solo habían producido “*serias averías e incendios que fueron sofocados inmediatamente, daños en tinglado y caseta consignatarios sin víctimas.*” (8). Al día siguiente el parte republicano informa de un ataque por parte de un hidroavión “Saboya” (9) al buque británico, al que lanzó varias bombas que tuvieron como consecuencia su hundimiento.

El final de la guerra.

Una vez acabada la guerra los destinos de los componentes de los grupos de criptografía y descryptado de ambos bandos fue muy diferente. En el bando nacionalista los principales miembros de estos grupos pasaron a formar parte del cuarto negociado (escucha, captación, criptografía y claves) de la Sección de información, curiosamente la tercera (10). En algunos casos, dado que no eran militares como Solabre, fueron asimilados a militares. Quedan en Madrid también varios miembros del grupo de descryptado del CTV, el Ufficio D, bajo el mando del teniente coronel Dragone, colaborando con los servicios de escucha y descryptación dirigidos por Antonio Sarmiento.

De los miembros de los servicios de descryptado republicanos, sabemos que Carmelo Estrada, después de ayudar a los franceses y de su paso por Argel, se exilió a Méjico, al igual que su hermano, Manuel Estrada, Jefe del Servicio de Información del Estado Mayor de la República. Del resto, Manuel Baringué volvió a España después de sufrir en sus carnes las condiciones infrahumanas en las eran tratados los españoles en el campo de Argelès-sur-mer. Del resto de sus miembros, después de su paso por los grupos de descryptado franceses Bruno y Cadix, se pierde su rastro y, lamentablemente, no volvemos a saber nada más (11).

Notas:

- 1.- En la referencia [1] puede verse una fotografía de una de estas máquinas y otra de un rotor con la numeración de la primera serie de las que se adquirieron a los alemanes.
- 2.- En la referencia [2] hay un estudio de las diversas máquinas de cifra utilizadas por el bando nacionalista en la guerra..
- 3.- Para saber más sobre los sistemas de cinta pueden verse, entre otras, las referencias [1], [3], [4], [5] y [6].
- 4.- Los miembros del grupo de descryptado en los últimos meses de la contienda, dirigidos por Carmelo Estrada Manchón (probablemente el Camazón del grupo BRUNO), eran César Vigas Vigas, Fernando Baringué Millat, Manuel Inglada Díaz, José Medina Cantero y José Díaz Rodríguez. Solo sabemos de la vuelta a España de Fernando Baringué, el resto, o al menos parte de él, debió formar parte del contingente de españoles que ayudaron a los franceses y polacos en la II guerra mundial en los grupos de descryptado BRUNO y CADIX.
- 5.- Véanse por ejemplo las referencias [7], [8] y [9].
- 6.- La historia viene descrita en [1] y en [10].
- 7.- Todos los descryptados presentados a continuación provienen del Archivo de la familia de José María Iñiguez.
- 8.- El Isadora fue posteriormente reflotado y bautizado como “Castillo de Frías”. Fuente: La marina italiana en la guerra de España. J. L. Alcofar Nassaes. Ed. Euros 1975.
- 9.- Tal como consta en el parte original, debía referirse a un hidro Savoia.
- 10.- El 30 de agosto (B.O.E. 243) se crea el Alto Estado Mayor con las funciones principales de

organización y preparación de las Fuerzas Armadas para su acción conjunta en caso de guerra. Éste se divide en tres secciones conocidas con el número de orden de la sección:

- Primera sección. Militar
- Segunda sección. Económica.

Tercera sección. Información.

11.- Gustave Bertrand, que fue el jefe de esos grupos dice en su libro "*Enigma ou la plus grande énigme de la guerre 1939-1945*", que se puso en contacto con el jefe del Servicio de Información Militar de la República, y con su hermano que era el jefe del servicio de descryptado, consiguiendo reclutar a los principales miembros de ese servicio (cinco oficiales), seguramente Carmelo Estrada y el resto de los miembros del servicio excepto Fernando Baringué.

Referencias:

- [1] Soldados sin rostro. Los servicios de información, espionaje y criptografía en la Guerra Civil española. José Ramón Soler Fuensanta y Javier López-Brea Espiau. Ed. INEDITA 2008.
- [2] Mechanical cipher systems in the spanish civil war. José Ramón Soler Fuensanta. Cryptologia vol. XXVIII, nº. 3. Julio 2004.
- [3] The Strip Cipher-The Spanish Official Method. José Ramón Soler Fuensanta y Javier López-Brea Espiau. Cryptologia vol. XXXI, nº. 1. Enero 2007.
- [4] Tratado de criptografía con aplicación especial al ejército. Joaquín García Carmona. Sucesores de Rivadeneyra 1894.
- [5] Los sistemas cifrados en la Guerra Civil Española. José Ramón Soler Fuensanta. Disponible en http://es.geocities.com/gce_euzkadi/paginas/cifra.html.
- [6] Missatges Secrets. José Ramón Soler Fuensanta. Editorial Mediterrània. Eivissa 2004.
- [7] La captura del Mar Cantábrico. José Luis Gordillo Courcières. Historia y Vida 313. Abril 1994.
- [8] Un Centro de Escucha y Descifrado en la Guerra Civil Española. José Ramón Soler Fuensanta y Javier López-Brea Espiau. Revista Española de Historia Militar 59. Junio de 2005.
- [9] De "Contrabandista" a Crucero auxiliar. El "Mar Cantábrico" en la Armada Española. Artemio Mortera Pérez, Lucas Molina Franco y Rafael A. Permuy López. Revista Española de Historia Militar. Abril 2001.
- [10] Russian and Soviet Cryptology. IV – Some incidents in the 1930'S. Tatyana A. Sobolyeva. Cryptologia Vol. XXV, Número 1, Enero 2001.