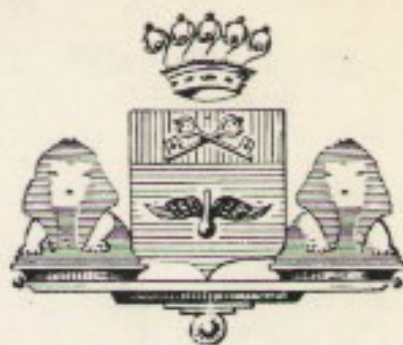




ASSOCIATION
DES
RÉSERVISTES
DU
CHIFFRE

Nouvelle Série — N° 3 — 1975

ESSAI D'HISTORIQUE DU CHIFFRE DE L'ARMÉE DE TERRE

(additif à la 3^e partie, publiée dans notre précédent numéro)

(1914-1919)

Un document fort intéressant se trouve au Service Historique des Armées, la note N° 6385/GQG du 6 mars 1918, parue sous le timbre commun du 3^e Bureau, de la Section du Chiffre, du Service Aéronautique et du Service Télégraphique (*), signée PETAIN. Cette note pour les Armées et Groupes d'Armées détaille les « procédés de chiffrement à employer aux différents échelons du commandement ». En fait, elle concerne surtout les petits échelons et ne parle pas du « vrai » Chiffre.

Elle comprend une introduction et trois parties. L'introduction explique que la généralisation de l'emploi de la T.S.F. et de la T.P.S. interceptables, impose des mesures de sécurité, pour éviter la compromission des codes, et d'adaptation aux moyens de transmissions. La première partie donne le détail des systèmes à employer, indépendamment des procédés spéciaux et des moyens sans dictionnaires, réservés aux Etats-Majors de Grandes Unités (il s'agit sans doute du SD 12) :

- un code chiffré en 3 chiffres
avec transmission directe par téléphone, pigeon-voyageur, avec surchiffrement à l'aide d'un tableau de concordance fréquemment variable et désigné par un nom d'animal, transformant les groupes de 3 chiffres en groupes de 2 lettres dans le cas de transmission par radio.
La transmission en code nu par le télégraphe est autorisée pour les messages ne concernant pas les opérations.
Ce système remplace le précédent code pour la T.S.F. dit P.P.H.

(*) Carton 16 N 1693 - pièce 13 871.

- des carnets réduits établis par les Armées, en groupes de 3 chiffres pour le téléphone, de 3 lettres pour la radio, la T.P.S. et l'optique ; on peut utiliser indifféremment chiffres ou lettres pour les pigeons.
- des listes N° 2 chiffrées pour l'observation aérienne, établies par les Groupes d'Armées et valables sur toute l'étendue de la zone du G.A.

Ces listes-codes sont en groupes de 4 lettres, la première étant caractéristique du tableau utilisé :

- des clés et bandes de chiffrement pour la transmission secrète des coordonnées. Il s'agit d'une substitution simple appliquée au premier chiffre de chaque groupe de 2 ; par exemple 72 — 84 devient M2 U4. Une clé est établie pour chaque carré de 2 km de côté.

La deuxième partie rappelle que le chiffrement est de la responsabilité des autorités, que c'est à elles de mettre en œuvre ces systèmes et non pas au personnel chargé de la transmission.

La troisième partie concerne les signaux conventionnels optiques ou sonores.

En conclusion, le commandant en chef prescrit que, dans tous les cours et stages quels qu'ils soient, une instruction doit être dispensée sur les dangers des interceptions adverses et sur l'emploi du Chiffre. Enfin il charge les 2^e Bureaux d'organiser un service d'écoutes amies pour veiller à l'observation des règles de sécurité.

»»»»««««

Essai d'historique *du CHIFFRE*

DE L'ARMÉE DE TERRE

(suite)

par L. RIBADEAU DUMAS



4^e PARTIE (1919-1939)

Cette période sera le prolongement de la guerre 1914-1918, avec une bonne application des enseignements recueillis ; cependant un effort sérieux de modernisation sera fait, freiné sans doute par une certaine timidité des chiffreurs, mais surtout, semble-t-il, par la méconnaissance par le Commandement de ses besoins réels. Le Chiffre se trouvera en 1939 dans une situation comparable à celle de l'Armée tout entière : les moyens existent, mais l'organisation et l'emploi n'ont pas suffisamment évolué, comme le montrera la période suivante 1939-1945. Et cependant une évolution était survenue dans les pays engagés, par la mise en service de machines mécaniques et électromécaniques qui remplacent largement les procédés manuels.

4-1. — ORGANISATION ET PERSONNEL.

4-1-1. — Au cours de la guerre, le problème de la place du Chiffre dans les états-majors s'était posé à plusieurs reprises, ainsi que celui de la subordination, au double point de vue du commandement et de la technique, et de la liaison avec ses fournisseurs (écoutes-gonio). Dès l'Armistice, le G.Q.G. entreprit de nombreuses études de réorganisation comme le montre un

ouvrage du Colonel PAOLI publié par le Service Historique des Armées (L'Armée française de 1919 à 1939 - La Reconversion). Grâce au Colonel PAOLI, un rapport fort instructif du 2^e Bureau du G.Q.G. a été retrouvé (carton 16 N 54 Pp 45) : étude sur l'organisation du 2^e Bureau N° 5987 du 29-3-19.

Cette étude remarque que le chiffre a deux objets : le chiffrement et le déchiffrement des télégrammes, le décryptement et l'exploitation des communications ennemies interceptées : « Tandis que le premier est à proprement parler un organe de courrier et correspond au service courant, le second constitue un organe de renseignement qui s'est révélé de plus en plus précieux au cours de la campagne ».

Le principe de la centralisation du renseignement conduit à conclure que ce second doit être partie intégrante du 2^e Bureau. Le « service courant » est à rattacher au service télégraphique, dont le personnel « par son recrutement même donne au point de vue du secret des communications toute garantie » (en 14-18, la grande majorité du personnel de la T.M. était du personnel des P.T.T. mobilisé).

En outre poursuit cette étude, cela « éviterait dans les états-majors des effectifs élevés pour le service de nuit ».

On peut dire que le 2^e Bureau tient à conserver la partie « noble », qui seule intéresse le renseignement mais veut se débarrasser du service courant, source d'ennuis et de la « corvée » des permanences de nuit !

Cependant cette étude n'oublie pas ce que nous appelons maintenant la direction du Chiffre (étude et choix des moyens, constitution des réseaux, contrôle du trafic chiffré) et confie cette tâche à la section de décryptement maintenue au 2^e Bureau, sans apercevoir le défaut majeur (qui se renouvellera, mais provisoirement en 1951) qu'est la séparation complète entre direction et exécution, entraînant la perte du sens des besoins et des réalités.

Cette étude propose les effectifs suivants :

- section de décryptement du G.Q.G. : 1 officier supérieur, 10 officiers subalternes, 6 sous-officiers, tous spécialistes du décryptement et un officier radiotélégraphiste (pour la liaison avec les éléments d'écoute et de radiogoniométrie).
- section de décryptement de l'Armée : 2 officiers ou sous-officiers.

Aucune section spécialisée n'est à prévoir aux autres échelons (G.A., C.A., Division), la direction du Chiffre devant sans doute y être exercée par les officiers du 2^e Bureau, et cela vient à l'encontre de ce qu'avait obtenu le Colonel GIVIERGE pour la diffusion de la « bonne parole » et du contrôle de la sécurité jusqu'aux plus petits échelons.

En ce qui concerne le « service courant », le 2^e Bureau propose pour l'échelon G.Q.G. 12 officiers ou 6 officiers et 6 sous-officiers.

Par « prudence » (sic) ce document ne proposait aucune modification à l'échelon du Ministre où elle proposait que la section demeure inchangée, avec la totalité de ses responsabilités du moment.

Aucune suite ne semble avoir été donnée à cette étude, dont le Colonel CARTIER put certainement montrer les lacunes ; son mérite était de mettre en lumière un certain nombre de points :

- importance du décryptement pour le renseignement ;
- ampleur des besoins réels (doublement des effectifs du G.Q.G.) ;
- séparation du Chiffre et du Décryptement ;
- distinction entre direction et exécution du Chiffre ;
- emploi des sous-officiers.

Mais elle eut jusqu'en 1940 une conséquence regrettable : l'effectif de la section du chiffre du G.Q.G. qui était de 13 ou 14 officiers fut ramené à 12, mais en lui maintenant la double tâche du service courant et du décryptement !

Cependant l'année 1921 voit une réforme fondamentale : au départ du Colonel CARTIER, promu général, la section du Chiffre quitte le Cabinet du Ministre et prend place au sein de l'E.M.A. ; elle dépend directement du chef d'état-major, mais, pratiquement, est aux ordres d'un sous-chef.

Dans ses souvenirs, le Colonel OLIVARI affirme avoir fortement influencé cette décision par la remise d'un mémoire au Général BUAT alors sous-chef d'E.M.A.

Avec le recul du temps, on peut penser que cette mesure était favorable à une meilleure satisfaction des besoins opérationnels ; le G.Q.G. s'était souvent plaint en 1914-1918 de ce que la section était trop lointaine et que ses préoccupations étaient

parfois trop éloignées des opérations. Par contre la section du Chiffre perdait son aspect « politique » ; la conduite de la guerre était délaissée, et cela peut expliquer la création ultérieure (42-43) d'organismes gouvernementaux prenant en charge d'une part la coordination des chiffres et d'autre part l'interception et le décryptement.

Aucune trace n'a pu être relevée d'une coordination interministérielle pendant cette période, en dehors des Armées. Les Affaires Etrangères continuèrent à faire bande à part, tandis que des liaisons existaient cependant entre l'Armée de Terre et la Marine, puis surtout l'Armée de l'Air à partir de sa création.

On peut aussi penser que devenue un petit élément de l'E.M.A., l'influence de la section sur le commandement demeura réduite, les préoccupations majeures des hautes autorités militaires étant autres, et le Chiffre continua à être un peu considéré comme un « empêcheur de tourner rond » (1). Ce rattachement à l'E.M.A. amena en particulier la suppression du bureau central de TSF et du rôle directeur de la section en matière d'écoutes et de radiogoniométrie. Ces tâches furent dévolues aux 2^e et 3^e Bureaux, comme elles l'avaient été pendant la guerre au G.Q.G.

4-1-2. — La nouvelle section de l'E.M.A. a les missions suivantes :

- chiffrement et déchiffrement des messages de l'Administration Centrale ;
- confection des codes et clés ;
- répartition des moyens (en accord avec le 3^e Bureau) ;
- études cryptologiques sur les chiffres, les inventions, etc... ;
- études et décryptement des chiffres étrangers et conservation des documents et renseignements y afférant (en liaison avec le 2^e Bureau) ;
- instruction des officiers d'état-major et des officiers de réserve du Chiffre.

(1) On peut citer, comme confirmation, la déclaration humoristique faite au banquet du congrès de 1938 des officiers de réserve du Chiffre, par un sous-chef de l'E.M.A. qui le présidait : « A ma connaissance, il n'existe que deux moyens pour arrêter efficacement une grande unité de cavalerie, pleine d'allant et de mordant : le premier, c'est de lui opposer une infanterie puissamment armée, appuyée par de nombreux chars, le second, c'est de l'obliger à chiffrer ses messages ! ».

Elle comprend environ 12 officiers et quelques sous-officiers utilisés comme secrétaires et comptables. L'atelier de chiffrement et de déchiffrement ne comprenait plus comme avant guerre de commis civils mais était constitué d'officiers, avec quelques sous-officiers secrétaires pour la dactylographie.

En 1919-1920, l'atelier comprenait 8 à 10 officiers, exploitant 80 à 100 télégrammes par jour, tandis que le décryptement était confié à 2 cryptologues, les Commandants PAULIER et BASSIERES.

En 1928, la sous-section « crypto » avait été considérablement renforcée et comprenait 8 officiers.

4-1-3. — Le Chiffre demeure affaire d'officiers, d'active et de réserve ; ces derniers sont environ 250 et occupent 95 % des postes « Chiffre » à la mobilisation. Ils sont recrutés uniquement par cooptation, dans la région parisienne, et font montre d'un dévouement et d'un zèle exemplaires.

Leur formation est assurée par un cours initial de 10 mois, comportant 20 séances et des travaux à domicile ; un cours d'entretien fonctionne régulièrement, dans le cadre de « l'Ecole de Perfectionnement du Chiffre ». Ils effectuent en outre des périodes de réserve assez fréquentes.

En temps de paix, il n'y a d'officiers d'active qu'à l'E.M.A. Dans les régions et grandes unités, l'exploitation du Chiffre est du ressort d'officiers d'état-major désignés localement à cet effet.

Les officiers d'état-major et les officiers des écoles d'application ont comme formation une ou deux conférences générales sur le secret et le Chiffre au cours de leurs stages ; elles sont cependant assez précises puisqu'une partie des renseignements donnés ici provient de conférences prononcées en 1927 et 1929, dont le texte a été conservé (1).

4-1-4. — Les tableaux d'effectifs « GUERRE », retrouvés au service historique fournissent les renseignements suivants :

(1) Le rédacteur de ces lignes se souvient d'une conférence du Colonel de France à l'Ecole Militaire et d'application du Génie en 1937, mais doit avouer n'avoir ressenti à l'époque aucun attrait particulier pour le Chiffre.

ECHELON	ANNEES					
	1920 à 1925		1926 à 1935		1936 à 1940	
	Officiers	Sous-Officiers	Officiers	Sous-Officiers	Officiers	Sous-Officiers
E.M.A. section chiffre	30 (8 OA 22 OR)	1 (plus secrétaires troupe)			30 (5 OA 25 OR)	3 (plus secrétaires troupe)
G.Q.G. (3 ^e Section du 2 ^e B.)	12	6	9	6	10	6
Cdt en Chef			2	2	2	2
Cdt en Chef AFN			2	2	1937 : 4 1939 : 9	4 3
Cdt en Chef Levant					1	2
Groupe d'Armées	2	1	2	1	2	1
Armée	1	1	3	1	3	1
Détachement d'Armée (1)			1	2	1	2
(1) Corps d'Armée Corps de Cavalerie et Régions fortifiées Groupement AFN	1	2	1	2	1	2
Divisions d'infanterie diverses (2)	0 (1920)	0 (en 1920)				
DC	1	3	1	2 3	1	2 1+8 HdR (3)
DLM (à/c 1934) D (1940)			1	1+8 (3)	1	1+8 (3) 1+5
Division aérienne	1	2	1	2		
Brigade aérienne	1	0	1	2		

NOTA :

(1) Ces T.E.G. précisent à partir de 1931 que ces personnels comptant à l'état-major seront détachés au commandement des Transmissions, mais il ne semble pas que cette « fusion » soit entrée en pratique pendant la guerre.

(2) A partir de 1932, les T.E.G. des D.I. comportent 3 officiers à l'E.M. de l'I.D., et précisent que ces 3 officiers doivent être aptes au chiffrement et au déchiffrement : remplacement de la section Chiffre, qui semble avoir été oubliée dans les T.E.G. de la division d'Infanterie motorisée de 1932 et 1936, ou renforcement éventuel en cas de gros trafic ?

(3) Contrairement aux autres T.E.G. où les hommes du rang, quand ils sont indiqués sont des ordonnances ou conducteurs, il semble que pour les D.C. et les D.L.M. on ait prévu l'accès au Chiffre des hommes du rang, puisque les T.E.G. précisent que ces effectifs sont destinés à mettre sur pied 3 ateliers et que seul l'un des hommes du rang peut être considéré comme ordonnance.

Certaines indications ont pu être obtenues sur la constitution des échelons A, c'est-à-dire de la fraction des unités mises en place en couverture en 1939 :

- G.Q.G. : 3 équipes de 1 O et 1 SO d'active plus 4 hommes du rang (3 ord. - 1 secrétaire) ;
- Armée : 1 officier d'active, provenant éventuellement de la G.R.M. et 1 sous-officier.

Pour le G.Q.G., le Groupe d'Armées et l'Armée, on indique qu'il y a un noyau d'officiers d'active provenant de la section, où ils sont remplacés par des O.R., et des officiers de Gendarmerie ou de la Garde Républicaine, solution déjà utilisée en 1914, ces officiers ayant suivi en temps de paix un stage de plusieurs semaines en 1938. On peut noter aussi que le nombre d'officiers prévus aux échelons C.A. et Division est très faible ; sans doute pensait-on les faire aider par des officiers non spécialisés de l'E.M. comme en 1914-1918, ce qui est prévu pour les D.I. (3 officiers de l'I.D.).

La composition des T.E.D. de 1939-1940 semble indiquer aussi que les sous-officiers pouvaient participer à l'exploitation du chiffre mais aucune décision « officielle » d'accès ne semble avoir été promulguée.

Vers 1927-1929, on envisageait de renforcer en cas de besoin les officiers par des sous-officiers « choisis », utilisés surtout comme secrétaires ; il semble qu'exceptionnellement, on ait pu admettre, en certains endroits, quelques sous-officiers d'active (origine chancellerie) au « secret du chiffre ». Les sous-officiers de réserve inscrits aux T.E.D. provenaient, eux, de la catégorie « secrétaires d'état-major » et il est certain qu'aucune instruction chiffre ne leur était dispensée.

A l'appui de cette présomption d'emploi de sous-officiers dans le Chiffre, on peut encore citer le Colonel GIVIERGE. Dans une conférence prononcée en 1929, peu avant son départ de la section et sa promotion au grade de Général, il indique deux possibilités futures : admettre des sous-officiers de confiance

dans le Chiffre, et autoriser les transmetteurs à chiffrer dans les centres de transmissions (!). Cependant il faut vraisemblablement admettre que ce n'était que pour le temps de guerre que cet emploi était prévu, sans avoir été officialisé. Le fait a d'ailleurs été confirmé par d'anciens officiers du Chiffre de 1939.

Et aucun renseignement n'a pu être recueilli sur les modalités d'emploi des hommes du rang pour les D.C. et D.L.M. à partir de 1932.

4.2. — LES MOYENS.

4-2-1. — C'est au cours de cette période que se produit la première révolution du Chiffre : l'introduction de machines mécaniques ou électro-mécaniques (la seconde sera celle de l'électronique, vers 1950).

La guerre 1914-1918 avait en effet fait ressortir la lenteur éprouvante des procédés manuels, mais aucun des appareils proposés, en général très ou trop simples, ne pouvait convenir.

La machine ENIGMA apparaît en Allemagne entre 1925 et 1930 ; c'est une excellente machine à clavier, à 3 rotors avançant comme les roues d'un compteur ; mais son exploitation est assez lente car le chiffrer doit noter par écrit la lettre qui s'éclaire à chaque frappe.

Le souci de la section, sous le « règne » du Colonel de FRANCE, est d'avoir des machines imprimant automatiquement le texte chiffré ou déchiffré sur bande, comme les appareils télégraphiques.

C'est alors qu'entre en scène Monsieur Boris HAGELIN, un suédois, qui vient proposer vers 1933 sa collaboration, avec des ébauches de machines susceptibles de donner satisfaction.

Il présente en 1935 la C.35, qui va donner naissance à la C.36 de l'Armée de Terre et à la C.37 de la Marine (1), machines purement mécaniques, puis il réalise en collaboration avec la section une machine électromécanique à clavier, la B.211. Sur des principes légèrement différents, ces machines opèrent une substitution à double clés, avec 26 ou 25 alphabets

(1) La C.37 de la Marine avait la particularité de remplacer une lettre claire par un bigramme chiffré, de façon à diminuer les risques d'erreurs et à faciliter les recherches.

parallèles et engendrent une clé de rang très longue, grâce à des roues clés à ergots mobiles à avancement régulier, toutes ensemble. Le chiffrement de la C.36 se fait à « l'allemande », ce qui permet un fonctionnement identique au chiffrement et au déchiffrement.

Les cryptogrammes sont présentés sur bandes, en tranches de 5 lettres ; l'espace entre les mots est chiffré, de façon que les mots soient séparés au déchiffrement.

Dans l'état des connaissances et des moyens de décryptement de l'époque, ces machines donnaient la sécurité souhaitée.

La C.36 permettait de réduire d'environ 2/3 le temps nécessaire au chiffrement ou au déchiffrement (20 minutes au lieu d'une heure pour un message de 100 groupes environ), la B.211 permettait une rapidité supérieure, environ le double, compte tenu des opérations de conditionnement.

En 1939, l'Armée de Terre sera équipée d'environ 2 000 C.36 et 115 B.211.

4-2-2. — Après la guerre 14-18, on continue à employer les mêmes systèmes à base de codes, avec des renouvellements fréquents ; on note des parutions de codes à 4 et 5 chiffres destinés aux grandes unités en 1919, en 1921 et en 1932. Ces codes existaient en assez grand nombre, étant destinés aux G.U. et aussi, semble-t-il, aux attachés militaires ; on en relève au moins 7 types différents en 1921.

Mais une question très étudiée après la guerre est celle du surchiffrement. Deux procédés sont sur la sellette : la clé additive et la transposition ; c'est celui-ci qui est retenu, aussi bien dans une notice de 1923 que dans celle du 1-7-24, qui semble rester en vigueur jusqu'à la guerre. Ces notices prescrivent :

- soit un surchiffrement par transposition simple ;
- soit un surchiffrement par transposition simple avec relevé initial de diagonales.

Des notices propres à chaque système prescrivent le procédé à employer ; la transposition à diagonales est toujours utilisée avec les dictionnaires à 5 chiffres destinés aux hauts échelons.

Les moyens utilisés sont les suivants :

- 1927 :
 - hauts échelons (jusqu'au C.A.) : dictionnaires désordonnés à 5 chiffres ;

- échelons moyens (Armée à Division) : codes désordonnés à 4 chiffres ;
- petites unités : carnets analogues à ceux de 14-18.
- 1929 :
 Le code des échelons moyens est renouvelé et s'appelle le code 67, avec une correspondance lettres-chiffres pour les transmissions par radio. Les carnets destinés aux petites unités portent la référence 333, mais ils sont en cours de remplacement par des répertoires d'une capacité maximale de 676 expressions, traduites par des bigrammes littéraux. Comme pour les carnets antérieurs, plusieurs types existent et l'on ne prévoit pas de surchiffrement.
- 1939 :
 - hauts échelons (attachés militaires, chefs de mission, etc.), B.211 et dictionnaires désordonnés en groupe de 5 chiffres, le procédé courant de surchiffrement est une transposition à diagonales (1).
 - échelons moyens : C.36 et codes ordonnés en groupe de 4 chiffres dont le surchiffrement continue sans doute à être fait comme en 1923 (1).

Ces codes sont :

- RA (1932) pour le territoire (4 chiffres ordonnés ou 4 lettres désordonnées),
- ATM pour l'Afrique du Nord,
- 69 pour les formations métropolitaines ;
- petites unités : carnets de chiffrement semi-ordonnés, de plusieurs modèles, avec emploi de clés additives courtes (9 à 13).

Le procédé manuel de secours destiné aux officiers de liaison, type SD 12, semble être resté en service, peut-être avec certaines variantes.

Les petites unités emploient aussi un répertoire de condensation, en trigrammes (ATA pour attaque, ENI pour ennemi, etc...) qui n'est ni du chiffre ni du camouflage, mais un système d'abréviation pour accélérer la transmission. On prévoit seulement un camouflage additif pour les coordonnées et les noms de lieux et

(1) Dans les années qui précédèrent la guerre, la transposition à diagonale excellente du point de vue sécurité, mais d'emploi difficile et très sensible aux erreurs de transmission, eut tendance à être abandonnée au profit de clés additives longues, souvent tirées du dictionnaire lui-même. On note aussi l'emploi généralisé de clefs-blocs de transposition, utilisée une seule fois, présentées sous forme de blocs de cartes-lettres et inviolables.

d'unités (codés au moyens de répertoires occasionnels en 3 chiffres ou lettres), chiffrés par une substitution simple à représentation unique : clef des nombres genre CAMION VERT, etc... Il semble aussi que le PLAYFAIR ait été utilisé.

Enfin les Transmissions sont dotées d'un code particulier, le code TTSTF, qui est l'aboutissement d'un certain nombre de variantes du code TSF de la guerre 1914-1918.

Il s'agit d'un code semi-ordonné en groupes de 4 chiffres, ayant un vocabulaire technique assez riche. Il est surchiffré par une substitution littérale simple à représentation multiple, tout l'alphabet étant utilisé. En outre, alors que le code TSF de la guerre 1914-1918 pouvait être utilisé pour des messages tactiques, le code TTSTF, qui était en service avant 1937, ne doit servir qu'aux messages techniques.

4-2-3. — Liaisons étrangères.

En 1939 sont mises en place en plus des liaisons d'attachés militaires ou de missions, des liaisons directes avec les commandements alliés, polonais (mission du Général HARTUNG avec le Commandant JOUBERT des OUCHES pour le Chiffre, le Capitaine COMBEAUX pour les transmissions) et britannique.

4-3. — L'ARMÉE DE L'AIR.

Lors de la création de l'Armée de l'Air, une section du Chiffre, analogue à celle de la Guerre est instituée à l'E.M.A.A. sous le commandement du commandant de DAMPIERRE, détaché à cet effet en 1934 ainsi que plusieurs autres officiers de la section de l'E.M.A.

Le Chiffre de l'Armée de l'Air est rapidement organisé, sur le modèle de l'Armée de Terre, équipé de codes et ensuite des B.211 et C.36.

Le Commandant de DAMPIERRE crée également un centre d'instruction pour officiers de réserve, qui est dirigé par le Capitaine BAUDOIN (1).

(1) Bien connu par son « Manuel de cryptographie » et disparu en 1943 en mer au cours d'une liaison aérienne entre LONDRES et ALGER.

4.4. — DECRYPTEMENT.

4-4-1. — Il n'existe pas comme pour la période précédente, d'archives ou de rapports précisant les résultats obtenus.

En outre un certain cloisonnement se produisit entre la section du Chiffre et le S.R., en partie pour des raisons de sécurité du renseignement, mais aussi, on ne peut le dissimuler, pour des questions de personnes.

Les informations données ci-après reposent sur des souvenirs et sur le livre du Général BERTRAND « La plus grande énigme de la guerre 39-45 ».

4-4-2. — La section du Chiffre poursuit son travail de la guerre.

En 1921, les Allemands utilisent pour tous les codes un UNIVERSALSCHLUSSEL ; c'est une substitution à double clé, qui ne semble pas avoir posé de difficulté majeure.

A partir de 1936, malgré la présence de plusieurs milliers d'ENIGMA, dont la mise en service régulier débuta en 1928, ils continuent à utiliser des codes et procédés qui seront assez bien connus en 1939.

- un code SD à 5 lettres ;
- des codes à 4 lettres ou chiffres ;
- un code à 3 lettres dans la LUFTWAFFE.

Ces codes sont en général surchiffrés par substitutions à double clé ou transposition. La police allemande utilisait une double transposition sur le clair et tous les télégrammes interceptés sont régulièrement décryptés.

En 1939, de nombreux codes étrangers (anglais, espagnols, allemands) étaient en partie reconstitués.

Comme pendant la guerre 14-18, les P.T.T. remettaient à la section tous les télégrammes chiffrés reçus ou expédiés et beaucoup étaient décryptés.

Il faut signaler aussi qu'au MAROC en 1933-1934, la section locale, sous la direction du Capitaine JOUBERT des OUCHES, réussit en la personne d'un de ses adjoints, le Capitaine PAS-COT, à reconstituer des clés espagnoles et à décrypter de nombreux messages, ce que le Résident et le Commandant supérieur apprécièrent beaucoup, car plusieurs centaines de messages furent lus de 1933 à 1936.

La section s'était attaquée à l'ENIGMA dès sa mise en service et cela donna lieu à divers décryptements réussis, mais le problème général était rendu difficile par la relative faiblesse du trafic.

A partir de 1937, un nouveau modèle fut mis en service, beaucoup plus complexe, comme nous le dirons plus loin et résista à toute tentative.

4-4-3. . . Depuis la première mise en service de l'ENIGMA (1926) les services de renseignements français tentaient d'obtenir des informations. Or, en 1932 un fonctionnaire allemand du service du Chiffre de la REICHSWEHR prend contact avec un attaché militaire, puis avec le S.R. et, pour des motifs vénaux, fournira jusqu'en 1939 des renseignements capitaux, que le S.R. va exploiter pratiquement seul. Il fournit des informations photocopiées sur les codes et procédés utilisés, sur l'ENIGMA et les clés employées et sur les décryptements allemands. On reconnaît ainsi les types successifs de l'ENIGMA :

- 1926 : modèle MARINE ;
- 1928-1930 : ENIGMA G ;
- 1930 : ENIGMA I ; ENIGMA II couplée avec une machine à écrire, qui donnera de mauvais résultats ;
- 1937 : ENIGMA type WEHRMACHT.

Les modèles de 1926 à 1930 comprenaient 3 à 5 rotors, avec anneaux de calage variables, le modèle 1937 ne comprenait que 3 rotors, mais le courant électrique traversait à nouveau le bloc de 3 rotors à l'envers, après une substitution réalisée par un jeu de fiches.

Le « correspondant » allemand fournira les jeux de clés de 1932, 1933, 1934, ainsi qu'une abondante documentation sur la machine.

Le S.R. français ayant appris que le S.R. polonais travaillait sur la question, un échange fructueux d'informations a lieu et les polonais réussissent peu avant la guerre de 1939 à reconstituer la machine et en donnent deux exemplaires au S.R. français, dont un pour les britanniques ; cette reconstitution de machine est à rapprocher de celle faite par les américains de la machine japonaise, également peu avant la guerre.

Le « correspondant » allemand fait aussi savoir que les services allemands de décryptement, dont les effectifs étaient de 60 pour l'Armée de Terre et 150 pour l'Armée de l'Air (sous l'impulsion personnelle de GOERING) avaient réussi à rétablir plus de 20

dictionnaires et codes étrangers : FRANCE 14, BELGIQUE 3, PAYS-BAS 2, SUISSE 3, divers 10.

Le S.R. de son côté s'était procuré des codes d'une dizaine de pays et il y eut une véritable « guerre » des codes, certains pays, dont l'ITALIE et l'ALLEMAGNE, faisant vendre des codes qui ne restent en service que pour justifier la vente et communiquer de faux renseignements.

Le Général BERTRAND signale entre autres faits que le S.R. italien avait une équipe de « visiteurs de coffres-forts » qui, en 1939, avaient visité les coffres de toutes les ambassades de ROME sauf celles du JAPON et de l'U.R.S.S., ce qui justifie la mesure prise par la section du Chiffre, indiquée au paragraphe 4-2-2 d'utiliser des clefs-blocs-une-fois incrochetales.

4-4-4. — On peut conclure que par les actions parallèles de la section du Chiffre et du S.R., la situation du décryptement français était assez favorable en 1939, encore qu'un procédé systématique de décryptement de l'ENIGMA n'ait pu, semble-t-il, être établi.

4-4-5. — Outre les renseignements donnés par le Général BERTRAND et résumés ci-dessus, quelques données donnent à penser que les services de décryptement allemand, beaucoup plus riches en personnel que les nôtres (3 à 4 fois au moins), avaient obtenu des résultats importants. Ils établirent en effet avec la société HAGELIN de bonnes relations qui se développèrent d'ailleurs après la guerre et se procurèrent 2 exemplaires de la machine C.35 proposée également par HAGELIN à la FRANCE (cf. § 4-2) (1). Il est vraisemblable que, de façon directe ou indirecte, ils obtinrent sur les machines C.36, C.37 et B.211 des informations qui leur permirent d'obtenir les résultats indiqués plus loin (§ 5-1-3).

4-5. — MOYENS DES AUTRES SERVICES FRANÇAIS.

A titre d'information, et pour comparaison, on notera l'existence des moyens utilisés par d'autres départements ministériels :

Ministère des colonies : on relève des codes analogues en 1903 (BMP), 1914, 1921, 1923, ce sont des codes semi-ordonnés,

(1) Source : Die deutsche Marine-Funkaufklärung de HEINZ BONATZ, Darmstadt 1970.

chaque page étant désignée par un trichiffre variable, les mots de chaque page étant identifiés par un bichiffre constant, utilisés sans surchiffrement.

Intérieur : en 1926, un code L 12, identique à ceux des colonies.

En 1927, on note un code PR 10 Istamboul, sans doute destiné à l'attaché militaire, semi-ordonné, à 4 chiffres (un bichiffre variable par page) mais avec obligation de surchiffrement, on ne sait si ce code venait de la section du Chiffre ou des Affaires Etrangères.
