ASSOCIATION DES RÉSERVISTES DU CHIFFRE

Nouvelle Série — N° 2 — 1974

Essai d'historique du CHIFFRE

DE L'ARMÉE DE TERRE

✱

Le Général RIBADEAU DUMAS (C.R.) a bien voulu nous réserver la primeur d'un travail entrepris à la demande de la direction centrale des Transmissions sur l'histoire du Chiffre de l'Armée de Terre.

Le début de ce travail, qui s'arrête à 1919, est à considérer comme du domaine historique public. La rédaction du bulletin de l'A.R.C. espère pouvoir publier la suite dans des bulletins ultérieurs.

L'auteur s'est volontairement limité aux données de l'histoire du Chiffre de l'Armée et de ce fait son texte pourra apparaître incomplet aux connaisseurs de l'ensemble du Chiffre que sont beaucoup de nos lecteurs. Il les prie de l'en excuser, ainsi que des incertitudes qui n'ont pu être levées ou des inexactitudes dues à une documentation fort difficile à rassembler.

—o—

PREAMBULE

Tenter d'écrire l'histoire du chiffre est une gageure.

La protection du secret du chiffre, qui conditionne celle des informations, a toujours entraîné la discrétion des initiés et la destruction des archives.

Les quelques éléments datant de plus de cent ans sont dus :

— à la découverte de textes chiffrés, conservés dans les archives à des époques où la sécurité était quelque peu relâchée, au point que le déchiffrement figure parfois en surimpression sur le cryptogramme ;

— à quelques indiscrétions des mémorialistes, malheureusement rares et souvent sujettes à caution.

A partir de 1889, nous disposons d'une étude du Général GIVIERGE, ancien chef de la section du chiffre du Ministère de la Guerre, qui s'arrête en 1916 ; elle est basée sur les archives de la Commission du chiffre, puis celles de la section, malheureusement disparues à ce jour (sans doute brûlées en 1940). Elle fourmille de détails, sinon sur les procédés employés, du moins sur la vie et les activités du chiffre de l'Armée de Terre.

INTRODUCTION

Les chefs de guerre, comme les politiques, ont toujours cherché à surprendre leurs adversaires sans être surpris par lui, de façon à créer et mener l'événement, comme le faisait l'Empereur.

Parmi les moyens utilisés à cet effet, le chiffre a tenu et tient une place importante, permettant de dissimuler la pensée contenue dans les textes et messages. C'est dans ce but que l'employaient jadis les souverains aux prises avec des voisins ambitieux ou des puissances dangereuses : oligarques et papes italiens de la Renaissance, rois et empereurs aux larges desseins comme Charles-Quint, Philippe II, Henri IV, Louis XIII, Louis XIV, etc...

Jusqu'à l'époque moderne, le rassemblement des forces sur le champ de bataille, ainsi que la brève durée des combats n'avaient pas imposé l'usage de transmissions indiscrètes en cours d'action (1) et le volume des informations à acheminer est longtemps demeuré faible.

Durant des siècles, le chiffre reste l'apanage de la diplomatie, des hauts niveaux de commandement. N'existe donc alors que le « chiffre de cabinet » destiné aux directives et informations d'importance majeure, échangées entre autorités de haut échelon.

Cette situation a été radicalement changée par les progrès techniques : les facteurs principaux sont l'accroissement du volume des informations à protéger et la généralisation des moyens de transmission électriques et électromagnétiques : multiplication et dispersion des autorités, besoin d'acheminement

---

(1) A l'exception peut-être de la Guerre d'Espagne, la campagne d'Allemagne de 1813, et celle de Waterloo, sous Napoléon.

toujours plus rapide de l'information, conséquences accrues d'un événement local, en lui-même de faible importance, mais dont l'exploitation rapide peut entraîner des résultats décisifs.

C'est pourquoi le chiffre s'est étendu et s'étend encore à des échelons toujours plus bas et à des correspondants toujours plus nombreux ; le « chiffre de cabinet » se dilate, devant s'appliquer à toute information, quels que soient sa nature et son niveau.

Le besoin, initialement simple et limité, s'est différencié dans son objet (texte, parole, image) et dans son niveau, faisant apparaître à côté d'un chiffre de cabinet toujours nécessaire des réseaux généraux et particuliers réclamant des degrés de sécurité plus ou moins grands.

Face à cette évolution des besoins, qu'a fait la technique du chiffre ?

Sur le plan des principes, tout était connu à la Renaissance et même bien avant, car il n'y a et ne peut y avoir que deux principes, la substitution où un élément clair est remplacé par un élément chiffré, sans que soit modifié l'ordre de succession de ces éléments (cas du chiffre de Jules César) et la transposition qui bouleverse l'ordre de succession des éléments, sans modifier ceux-ci (cas de la scytale grecque).

Tout procédé du chiffre découlera de ces principes, employés isolés ou combinés, selon des règles de modification pouvant varier en cours d'action.

Ce sont ces règles qui donneront naissance aux divers systèmes de chiffrement (1) employés d'abord manuellement (crayon-papier selon la terminologie usuelle), l'exécution de ces systèmes fut confiée ensuite à des machines mécaniques ou électromécaniques et c'est maintenant à des ensembles électroniques automatiques, pouvant associer chiffrement et transmission et dans certains cas saisie et diffusion de l'information.

C'est cette évolution du chiffre français que nous tenterons de décrire dans les pages suivantes, dans son organisation et dans sa technique.

Une dernière remarque s'impose : dès l'origine, nous voyons chiffrement et décryptement étroitement liés, centralisés au

(1) Nous n'en décrirons pas ici, renvoyant le lecteur aux manuels classiques, BAUDOIN, GIVIERGE, SACCO, etc...

plus haut échelon, confiés aux mêmes cryptologues ; ce n'est qu'après 1943 qu'ils ont été dissociés en France, alors qu'ils restent unis dans tous les grands pays.

»»»«««

PREMIERE PARTIE

DE L'ORIGINE A 1871

Peut-on citer au titre du chiffre le code des signaux lumineux utilisés par les Gaulois ? L'on trouve dans des textes anciens des noms de lieux ou de personnalités remplacés par des sobriquets convenus plus ou moins transparents, époques de Philippe le Bel, de Charles V ainsi que de François I[er] et des guerres de religion.

Auparavant même, Chrétien de Troyes cite des textes symboliques, connus des seuls initiés, des échanges d'objets dont le sens était préétabli, et les maîtres maçons utilisaient des graphismes conventionnels, de même que les Templiers, gitans, etc...

Sans doute aussi Catherine de Médicis introduisit le chiffre dans sa correspondance, mais c'est au XVII[e] siècle que l'on peut fixer l'acte de naissance officiel du chiffre français, avec une organisation qui subsistera jusqu'après la Révolution et l'Empire.

Le chiffre fait partie du « Secret du Roi ». Les chiffreurs sont des commis civils peu nombreux, des « domestiques » ignorés comme le sont restés aussi les agents chargés de renseignement ou de missions spéciales (1).

C'est d'abord la grande époque des VIGENERE (Henri IV), VIETE (Louis XIII), et ROSSIGNOL (Louis XIII et Louis XIV), le premier faisant après TRITHEME, la théorie de la substitution à double clé, et le dernier créant le grand chiffre de Louis XIV.

En fait, on n'utilisera dans la période considérée que la substitution simple, avec une représentation multiple éventuelle pour certains éléments fréquents, sous forme de tableaux.

(1) Qui sait qu'après Louis XV, Napoléon utilisait des agents spéciaux pour certaines négociations, tels son chambellan THIARD (nommé général à la Restauration) pour conclure le mariage du Prince EUGENE avec la princesse Auguste de BAVIERE et celui de l'héritier de Bade avec Stéphanie de BEAUHARNAIS.

Certains seront désordonnés, en particulier sous la Monarchie au XVII[e] siècle mais la décadence apparaîtra au XVIII[e] siècle par l'abandon de cette judicieuse précaution que l'on ne retrouvera que dans les répertoires et dictionnaires du XX[e] siècle.

Sous Louis XIV, le grand chiffre comportait des tableaux de 600 groupes, le petit chiffre 300 seulement.

Sous Louis XV, les tableaux ont 900 ou 1 500 groupes mais on a relevé une table avec 6 000 groupes !

Sous Napoléon, le « GRAND CHIFFRE » n'avait que 182 groupes, mais les besoins de la géographie et de la logistique portèrent jusqu'à 3 000 certaines tables.

Ces tableaux assuraient théoriquement une sécurité suffisante, car le volume de la correspondance était faible, ils ne concernaient en général qu'un théâtre d'opérations et étaient changés à chaque campagne. Il y avait même parfois plusieurs tableaux utilisés selon le destinataire (chiffres particuliers du Roi et du Ministre, dans certaines campagnes de CATINAT).

Néanmoins on a pu opérer des décryptements au XVII[e] siècle (VIETE puis ROSSIGNOL perçant le chiffre espagnol) et surtout, depuis 100 ans, les cryptologues français ont restitué nombre de cryptogrammes du XVII[e] siècle et de l'Empire.

Les raisons en sont le mélange habituel du clair et du chiffré, permettant de deviner certains mots, la connaissance par les cryptologues modernes des faits historiques en cause, fournissant des « mots probables » ainsi que la possession de certains documents où figurent, juxtaposés, clair et chiffré.

L'organisation du Chiffre était centralisée ; à l'origine, conception et utilisation (à l'échelon central) étaient confiées à des commis civils appartenant au « Secret du Roi ». Ce personnel était également employé à l'interception des lettres confiées à la poste ; ils les ouvraient et les refermaient sans laisser de trace, grâce à des techniques éprouvées, puis en remettaient copie, après décryptement éventuel, au Roi et aux ministres intéressés. C'est d'ailleurs à LOUVOIS que l'on doit l'organisation ou plutôt le développement et la systématisation de ce « service ».

On dit aussi que ces commis se succédaient de père en fils, et appartenaient à un petit nombre de familles, victimes faciles à trouver et à châtier en bloc en cas d'indiscrétion.

Le Chiffre servait pour les communications diplomatiques et militaires, étroitement liées sous la Monarchie, mais il est pro-

bable qu'il y avait au moins deux services distincts, l'un au Ministère des Affaires étrangères, l'un au Ministère de la guerre, au XVIII[e] siècle.

On a évidemment encore moins d'informations sur ces commis du Chiffre que sur ceux qui organisaient les mouvements des troupes et en particulier les concentrations au début de chaque campagne.

Aux échelons subordonnés, le Chiffre était exploité par les autorités elles-mêmes, ou, plus généralement, par des secrétaires ou des officiers, le plus souvent volontaires, attachés à leurs personnes.

A la fin du XVIII[e] siècle, l'Armée et le Ministère furent réorganisés par le Maréchal de BROGLIE, et ses réformes durèrent, semble-t-il, jusqu'après 1871. C'est à lui que l'on doit le « Dépôt de la guerre » qui constituait en fait à la fois l'état-major et le service géographique centraux, étroitement imbriqués et liés avec le Génie. On cite parmi les personnalités de ce dépôt des ingénieurs géographes, comme BERTHIER le père, le général SANSON et BACLER D'ALBE, qui furent les géographes de l Empereur, des officiers d'état-major comme BERTHIER, qui servit sous ROCHAMBEAU et son frère. Mais il ne semble pas que le Chiffre ait été rattaché à ce Dépôt ; il dut rester indépendant, dans l'entourage immédiat du Ministre.

Sous l Empire, BERTHIER ne paraît pas s'être beaucoup soucié du Chiffre ; il mit par contre tous ses soins au service des estafettes multiples ; beaucoup tombèrent entre les mains de l'ennemi en particulier en Espagne, où WELLINGTON sut fort bien utiliser les textes clairs ou chiffrés qui lui parvinrent, en Allemagne en 1813 ou en France en 1814.

On sait qu'il y avait du chiffre entre l'Empereur et ses corps détachés comme, en 1813, NEY et les forteresses conservées telles que MAGDEBOURG, mais on ignore qui avait la responsabilité de la conception.

Le manuel d'état-major du général baron THIEBAUT, si précieux à maints égards, puisqu'il restera le bréviaire des officiers d'état-major jusqu'après 1871, est muet sur le chiffre, ce qui tendrait à faire croire qu'il n'était pas de la responsabilité des états-majors, même si les officiers des états-majors l'utilisaient. Cependant ce même général raconte dans ses Mémoires qu'une de ses premières préoccupations, lorsqu'il fut nommé chef d'état-major de DAVOUT en 1813, fut de mettre en place des moyens de chiffrement (sur lesquels il ne donne malheureusement aucun détail) entre lui et les divisions subordonnées.

Les informations sont encore plus rares sur l'organisation du Chiffre sous la Restauration, LOUIS-PHILIPPE et le Second Empire où la routine et la décadence s'accentuent.

Lors de la conquête d'ALGER, BOURMONT avait un Chiffre avec Paris ; on a dit que c'était un code à 4 chiffres, semi-ordonné, la numération des pages, par bichiffre, pouvant changer à volonté ; ceci dénoterait un progrès notable, par rapport aux tables classiques de l'époque, mais ce renseignement n'est pas certain. Le même BOURMONT utilisait quelques années plus tôt, lors de l'expédition d'Espagne, pour sa correspondance personnelle avec son ami le ministre de la Marine, un chiffre hiéroglyphique (sans doute simple et analogue à ceux des francs-maçons et carbonari), pour dire du mal de ses chefs, du gouvernement de FERDINAND VII et de l'ambassadeur français à Madrid, dont le duc d'ANGOULEME n'était guère satisfait non plus !

Le Maréchal de CASTELLANE, commandant en chef de l'Armée de Lyon de 1850 à 1864, avait la responsabilité d'une sorte de grande région militaire et des troupes qui y étaient stationnées. Il raconte dans ses Mémoires qu'en 1855, le Maréchal VAILLANT, ministre de la guerre, lui adressait des dépêches chiffrées, relatives aux désignations de troupes pour la CRIMEE, et qu'il y répondait en clair, estimant qu'il n'y avait pas de secret à garder !

En 1859, en Italie, Napoléon III ne disposait que de deux tables très succinctes, respectivement de 155 et 234 groupes, qui avaient déjà servi en CRIMEE et comprenaient des désignations géographiques de cette campagne !

En 1870, BAZAINE se plaignait de l'insuffisance du vocabulaire de son tableau qui ne comportait ni le mot Infanterie, ni le mot Artillerie.

On peut ainsi constater que le Commandement, dans cette première partie du XIX[e] siècle, n'a accordé que peu d'intérêt au Chiffre, et que les résultats en furent regrettables. Le service d'état-major n'était pas mieux traité. Depuis la Restauration, les officiers d'état-major avaient eu une bonne durée de formation (1 an) et des avantages de carrière notables, mais c'était, comme pour le Chiffre, un fonctionnaire civil qui dirigeait le service (Ecole d'application et gestion du personnel).

En ce qui concerne le décryptement, un incident amusant, relaté par le Maréchal de CASTELLANE dans ses Mémoires, peut éclairer sur son organisation au début du XIX[e] siècle. Le

« cabinet noir » institué par LOUVOIS fonctionna sous l'Empire et la Restauration comme sous la Monarchie ; il fut supprimé par POLIGNAC (qui l'eût cru !) rétabli par LOUIS-PHILIPPE, suspendu en 1847 et sans doute remis en action par NAPOLEON III. Son existence était connue et vers 1835 comme sous l'Empire, on se plaignait que les interceptions des lettres diplomatiques ne donnaient aucun renseignement utile, les ambassadeurs utilisant d'autres moyens que la poste pour leurs courriers à protéger !

Le Chancelier PASQUIER rapporta au Maréchal l'anecdote suivante : il était ministre des Affaires étrangères, ce qui situe l'incident en 1820 ou 1821 ; le chef du Chiffre des Affaires étrangères, nommé CAMPI, avait inventé un « petit chiffre » qu'il jugeait indécryptable et à chaque nomination d'ambassadeur, proposait sa mise en service.

Il le proposa à nouveau au Ministre alors que se trouvait dans son bureau M. de MEZY, directeur général des Postes. Celui-ci demanda à M. CAMPI de chiffrer une dépêche fictive dont il garderait le clair et lui remettrait le chiffré. Deux jours après, M. de MEZY remettait le texte déchiffré au chancelier PASQUIER. M. CAMPI en fut fort marri. Ceci montre qu'il y avait des cryptologues au « cabinet noir », que le chiffre des Affaires étrangères, comme ceux de la Guerre et de la Marine étaient indépendants et sans doute sans relations avec ces cryptologues.

L'élément « décryptement » du cabinet noir semble avoir disparu plus tard, puisque le ministère de l'Intérieur fit appel, sous la 3e République, au commandant BAZERIES pour décrypter la correspondance du comte de CHAMBORD.

»»»«««

DEUXIEME PARTIE

DE 1871 A 1914

2-1. — Le renouveau des études militaires s'étend au Chiffre, avec quelque retard sans doute puisque ce n'est qu'à partir de 1902 que des résultats apparaissent.

On relève d'abord l'existence d'un cryptographe modèle 1886, appareil composé de 10 réglettes portant chacune des nombres différents, écrits en divers ordres sur leurs quatre faces,

mises en place d'après une clé et fournissant ainsi un tableau de transposition ayant autant de cases que de nombres sur les 10 réglettes. Le système fournissait plus de 3 600 milliards de tableaux distincts. Cet appareil peut se comparer dans son mode de réalisation au cryptographe BAZERIES, qui reposait, lui, sur la substitution à double clé, mais il ne fut sans doute pas plus utilisé.

Cette réalisation ingénieuse montre que les éléments techniques ne manquaient pas. On peut en effet noter à cette époque, outre le nom du Commandant BAZERIES, faisant de la cryptographie le violon d'Ingres, rémunéré, de sa retraite (il travaille pour l'Intérieur et les Affaires Etrangères) ceux des capitaines VALERIO et de Monsieur KERCHOFFS, dont les publications attiraient l'attention.

2-2. — ORGANISATION.

Ce n'est qu'en 1889 qu'on trouve la trace de la Commission du chiffre de l'Armée de Terre, qui, après quelques vicissitudes, devient permanente en 1894.

Dès lors, jusqu'en 1902, elle sera présidée par le Général inspecteur de la télégraphie militaire, puis par le général BERTHAUT qui fera faire des pas décisifs, enfin par le général de CASTELNAU et le général BERTHELOT.

Initialement les membres de cette commission avaient tous d'autres fonctions et ce n'est qu'en 1903 que l'un d'eux, le chef de bataillon du Génie CARTIER, son secrétaire, sera affecté à temps plein mais il aura aussi d'autres fonctions concernant la télégraphie militaire, au bureau central de T.S.F.

Le principe de la création d'un bureau de déchiffrement avait été retenu en 1899, mais sans suite, et ce n'est qu'en 1912 qu'il sera créée la section du chiffre, au Cabinet du Ministre, avec pour mission le chiffrement et le déchiffrement des messages, d'une part, les études de cryptologie et le décryptement de l'autre.

Deux ans avant la grande guerre, une structure efficace était enfin réalisée, mais les moyens en personnel étaient faibles et si la tête existait, elle n'avait pas de membres, aucun spécialiste n'étant prévu aux tableaux d'effectifs des états-majors, où la commission tentait cependant d'essaimer avec ses membres affectés fors de Paris.

Le mérite de cette progression revient au général BERTHAUT, qui présida la Commission pendant 10 ans, après en

avoir été membre et secrétaire pendant huit ans mais surtout au capitaine puis commandant CARTIER qui fut la « cheville ouvrière de ce développement grâce à son zèle et à son esprit d'apostolat » (GIVIERGE) et dont le caractère « diplomatique » et la ténacité permirent d'obtenir un succès certain.

Il faut signaler également que GIVIERGE, dans ses mémoires, dit qu'entre 1912 et 1914, la section du chiffre a bénéficié de la protection du chef d'état-major (Général JOFFRE) et de son appui efficace auprès du cabinet du Ministre.

En outre CARTIER eut à s'occuper de toutes sortes de tâches d'organisation et de liaisons, ce qui l'obligea à délaisser parfois le travail technique interne (ce que certains lui reprocheront toujours). C'est ainsi qu'il participa à l'établissement des liaisons franco-russes et franco-anglaises et surtout au développement de la T.S.F.

Dès 1899, le Ministère de la guerre se préoccupe de la liaison et de la collaboration interministérielles. L'accord, d'abord tacite, de la Marine et de l'Intérieur, (où existait un service actif dirigé par Monsieur HAVERNA, inspecteur des Renseignements généraux, survivance du « cabinet noir ») sera acquis officiellement en 1908.

Malgré la résistance des Affaires étrangères (Monsieur WILLIAM MARTIN, chef du bureau du chiffre), une commission interministérielle sera créée par décret du 9 janvier 1909. Elle comprend des représentants de l'Intérieur, de la Guerre, de la Marine, des Colonies et des P.T.T., sous la présidence du président de la Commission de la guerre ; le commandant CARTIER étant son secrétaire.

Dès 1907, la collaboration avait été excellente entre la guerre et l'Intérieur où Monsieur HAVERNA obtenait d'excellents résultats ; par contre les difficultés ne cessent pas avec les Affaires étrangères, dont les connaissances et les travaux sont pour le moins incertains.

La commission interministérielle ne se réunira d'ailleurs officiellement pour la première fois qu'en 1912, mais elle entérinera la remise par les P.T.T., des télégrammes chiffrés aux services intéressés et une certaine division du travail.

2-3. — TRAVAUX.

Les travaux de la commission du chiffre de la guerre porteront durant toute cette période sur :

— la création des moyens de chiffrement,

— la formation du personnel,

— le rassemblement des connaissances et le décryptement de systèmes étrangers.

2-31. — Le cryptographe à transposition modèle 1886 est abandonné ; si jamais il fut utilisé. De 1889 à 1912, il n'est question que de dictionnaires codiques ordonnés, dont la pagination pouvait changer, les mots fréquents étant décalés et ayant dans certains plusieurs représentations, ces deux dernières dispositions ayant été appliquées de façon systématique à partir de 1899. Il semble que leur vocabulaire ait atteint au maximum 8 000 éléments à 4 chiffres (100 pages de 80 groupes).

La sécurité était donc assez faible, surtout pour les premiers, techniquement en retard sur les tableaux désordonnés du siècle de Louis XIV, mais elle était suffisante, compte tenu de l'emploi assez réduit et de la fréquence de leur renouvellement.

On trouve en effet, pour les hauts échelons, des dictionnaires type I (paix) et type II (guerre), édités en 1890, 1903, 1913 et pour les échelons subordonnés des types A et B guerre en 1895, 1903 et 1913.

La recherche d'un système littéral sans dictionnaire n'était pas oubliée ; après des refus en 1894 (substitution à double clé) 1902 et 1908 (substitution simple à 4 représentations suivie d'une transposition) était adopté en 1912 un système à transposition à diagonales, avec un tableau d'abréviations. Ce procédé sera d'ailleurs cher à notre section du chiffre, puisqu'un système analogue sera encore en service en 1945 (pour le surchiffrement d'un dictionnaire, il est vrai).

On réalisera aussi un dictionnaire franco-russe en 1912 et un dictionnaire franco-anglais en 1913.

2-32. — Le problème de la formation de personnel se pose dès l'origine, mais ce n'est qu'en 1902 que le général BERTHAUT et le commandant CARTIER parviennent à obtenir les premiers moyens.

Des officiers de la garnison de Paris peuvent suivre des cours et, après un petit examen, 3 sont retenus (sur 10 candidats) qui, dans la mesure de leur temps libre, car ils conservent leurs affectations et leurs tâches correspondantes, se formeront et participeront aux travaux de la Commission.

Ce système continuera jusqu'en 1914, les officiers formés à Paris continuant à participer aux travaux dans leurs affectations de province (le commandant CARTIER n'obtiendra en général pas leur maintien à Paris).

La situation ne s'améliorera un peu que lors de la création de la section du chiffre, en 1912, par l'affectation de quelques officiers.

Les efforts déployés pendant cette période auront permis de créer un noyau compétent et passionné de cryptographie.

Les problèmes de la sécurité et du chiffre seront aussi évoqués dans des conférences faites à partir de 1904, semble-t-il, à l'Ecole supérieure de guerre et ensuite dans les états-majors de corps d'armée.

Cependant un déficit important subsiste face aux besoins réels dont le commandement ne s'est pas aperçu. L'emploi d'officiers surnuméraires ou de réserve, avait été envisagé et avait touché 2 ou 3 officiers dont la trace se perd rapidement.

2-33. — Pour former ce personnel, nécessaire à la conception du chiffre, à son exploitation et au décryptement, il fallut rassembler les connaissances éparses, inventer des méthodes et procéder à des exercices et travaux réels de décryptement.

A partir de 1902, un travail efficace est entamé ; auparavant on ne cite que quelques exercices de chiffrement et de déchiffrement, en 1896, pour le personnel qui en avait la charge.

Le colonel BERTHAUT et le commandant CARTIER organisent des cours pour les 3 élèves admis, cours reposant, semble-t-il, sur des exercices de décryptement de systèmes simples. On s'attaque aussi aux chiffres étrangers et les premiers résultats acquis en 1904 concernent un procédé allemand, en transposition simple, et un italien, en substitution à double clé, mais ces travaux sont interrompus, faute de personnel.

Ils reprennet en 1906, lorsque la fusion du chiffre et du décryptement est obtenue et on attaque en particulier les systèmes à base des dictionnaires civils couramment utilisés dans le monde entier (SITTLER, BAZERIES, un italien etc...).

Un travail très important est fait également par Monsieur HAVERNA sur des cryptogrammes étrangers, en particulier de 1907 à 1912 avec l'aide de GIVIERGE qui a quelques connaissances en russe.

Mais les affaires étrangères refusent de tenir compte de ces résultats et d'y apporter leur aide, conservant jalousement le secret sur leurs possibilités qui font l'objet de déclarations contradictoires de leur part.

En somme en 1914, les matériaux nécessaires sont rassemblés ; on a réussi à entrer dans deux chiffres étrangers, on a arrêté les procédures permettant d'obtenir rapidement des cryptogrammes, par les P.T.T. ou les écoutes T.S.F., mais ce n'est qu'un commencement, la « machine » est incomplète et n'est pas rôdée.

NOTA : Voir annexe à la fin de l'article.

»»»«««

TROISIEME PARTIE

LA GUERRE 1914 - 1918, 1919

3-1. — La guerre 1914-1918 va voir se développer l'organisation et les procédés créés avant guerre : l'évolution se poursuit lentement, mais le chiffre reste toujours l'apanage d'un très petit nombre d'hommes qui réussissent à maintenir le secret et fournir de nombreux renseignements par le décryptement et le déchiffrement des messages ennemis, certains d'importance capitale pour la conduite des opérations. On reconnaît la nécessité du surchiffrement des codes et dictionnaires (1916), tandis que de nombreux procédés de l'ennemi ou de neutres ne résistent que peu aux décrypteurs dont l'habileté croît avec l'expérience.

3-2. — ORGANISATION.

3-21. — A l'époque moderne, compte tenu du volume toujours croissant du trafic chiffré, organes de direction et d'exécution sont séparés. Pendant la guerre 1914-1918 et plus de 30 ans encore après, ils demeurent confondus. Aux échelons les plus bas, par contre, des non-spécialistes occasionnels seront chargés du chiffrement et du déchiffrement. Dès fin août - début septembre 1914 les organes du chiffre ont pris l'organisation qui demeurera, sauf très légères modifications, jusqu'à la fin des hostilités.

3-22. — A la tête, la Section du chiffre, rattachée au cabinet du Ministre, dont les attributions sont :

— direction du chiffre de l'armée de terre : création des systèmes, organisation des réseaux, préparation et gestion des documents - contrôle de l'exécution ;

— rassemblement des éléments concernant les chiffres étrangers, décryptement de systèmes - déchiffrement de messages ;

— chiffrement et déchiffrement des messages du Ministère.
— bureau central de T.S.F.

S'y ajoutera pendant quelque temps en 1914 un bureau chargé de la collecte et de la diffusion des télégrammes radios ennemis en clair, mais cette charge sera rapidement écartée. En dehors des attributions proprement « Chiffre » il y a celle du bureau central de T.S.F., créé avant guerre et donné au commandant CARTIER (ancien officier du 24° bataillon du Génie, ancêtre du 8° régiment du Génie).

Ce bureau a pour mission l'organisation générale des grandes liaisons radios, en particulier avec l'étranger et les Territoires lointains. C'est une amorce de Commandement des Transmissions de l'Administration centrale, habilité uniquement pour la radio, mais il en a les attributions : organisation des liaisons et réseaux, fourniture des indicatifs, des adresses, fixation des vacations, etc... avec en outre la fourniture des documents du chiffre.

Un nouveau bureau est créé en 1915 : ses attributions sont l'organisation générale du système radiogoniométrique et l'exploitation de ses résultats. La radiogoniométrie avait en effet réalisé rapidement des progrès remarquables, mais l'exploitation de ces résultats demandait une bonne connaissance de l'organisation des réseaux adverses, des indicatifs (variables), avec la correspondance entre P.C. et indicatifs, des systèmes d'exploitation et de chiffrement utilisés, etc..., et ce n'était qu'à la section du Chiffre que tous ces éléments étaient réunis.

3-23. — Tant que dure le « règne » du général JOFFRE, le G Q G a pratiquement compétence sur l'ensemble de l'Armée de Terre. Il dispose d'une section du chiffre, placée dès la mobilisation sous le commandement du chef d'escadrons GIVIERGE. Cette section rencontre dès l'abord des difficultés de rattachement, d'abord indépendante, puis adjointe au bureau du courrier, puis rattachée au 2° bureau, alors qu'elle sert en fait tout l'état-major. Elle souffre à plusieurs reprises de cette subordination, mais peut en fait conserver une autonomie pratique de fonctionnement.

Toutefois la personnalité du chef du 2° bureau, et celles de certains officiers de ce bureau ont une influence parfois néfaste sur les décisions d'organisation prises à l'échelon d'un sous-chef d'E-M, mais à partir de 1916 la situation est bien assise et les conditions de fonctionnement satisfaisantes.

Le principal travail de cette section était :
— la direction du chiffre des Armées : création des réseaux,

mise en place et gestion des moyens, instruction, contrôle de l'exécution ;

— le chiffrement et le déchiffrement des messages émis,

— le déchiffrement de messages de l'adversaire au moyen des clés fournies par la section du chiffre du Ministère.

Il n'y a pas de spécialisation ; chacun participe plus ou moins aux diffférentes tâches, sous la direction du chef de section et en fonction de ses aptitudes et du travail du moment.

L'ensemble du personnel œuvre en effet en brigades, de façon à assurer un service continu ; la priorité est donnée au chiffrement et au déchiffrement des messages.

3-24. — A l'échelon des groupes d'Armées et Armées, une note du Major général du 17 septembre 1914 crée un bureau du chiffre comprenant 1 officier et 1 adjoint ; une seconde note du 14 octobre 1914 prévoit plusieurs adjoints et des dispositions relatives au service du chiffre dans les missions à l'étranger et auprès des armées étrangères.

En fait le chiffre a beaucoup de difficultés à s'implanter et à fonctionner dans de bonnes conditions dans les diverses Armées. Comme le dit GIVIERGE, « dans les Armées, le chiffre n'était point aimé, et le G Q G ne l'était guère ».

Aussi, surtout dans les périodes du début de la guerre où le trafic chiffré est faible, les chefs d'état-major donnent d'autres fonctions à leurs officiers du chiffre, les rattachent au bureau du courrier ou à un autre (1° ou 3°) etc... De très nombreuses difficultés apparaissent ainsi tout le long des années 1915 et 1916, en particulier à la 2° armée (commandée par le général PETAIN).

L'affaire était d'autant plus délicate qu'il fallait aussi désigner dans les E-M des « suppléants » pour remplacer l'officier du chiffre en cas d'absence, et lui permettre de dormir ; cette corvée supplémentaire ne plaisait guère aux suppléants, qui devaient s'instruire et ne manquaient pas de recevoir observations et semonces quand ils se montraient trop lents ou commettaient des erreurs.

Peu à peu les difficultés s'aplanissent cependant, en particulier lorsqu'il faut doter les unités en ligne de moyens de camouflage contre les interceptions téléphoniques ou radiotélégraphiques. La fonction de direction de l'officier du chiffre s'affirme alors et l'habitude se prend de le rattacher au 2° bureau. Mais il reste toujours l'impression que les officiers du chiffre sont des

« planqués » dans leurs tours d'ivoire et n'ont rien à faire. Leur rôle, de rappel des règles de sécurité, les fait aussi, déjà, prendre pour des empêcheurs de tourner en rond (euphémisme !).

3-25. — Aux échelons subordonnés aux Armées, corps d'Armée et divisions, et dans les régions militaires, il n'y a pas d'officier du chiffre spécialisé, et le chef d'état-major a à désigner un officier et des suppléants pour recevoir et gérer les documents, chiffrer et déchiffrer les messages. Font exception les corps d'Armée de cavalerie où il y a 1 ou 2 officiers spécialisés.

3-3. — EFFECTIFS ET PERSONNELS.

3-31. — Il n'a pas été possible de retrouver de T.E.D., si jamais il en a existé ; les effectifs ont dû être fixés par notes internes ou accordés verbalement.

La Section du Chiffre du Ministre, comme celle du G Q G ont été portées très rapidement, en moins d'un mois après la mobilisation à leur effectif de croisière :

3-311. — La section du Chiffre du Ministre comprenait principalement :

— son chef : le chef de bataillon puis lieutenant-colonel, puis colonel CARTIER ;

— un élément de secrétariat chargé aussi de la confection des dictionnaires ;

— 1° Bureau : chiffrement et déchiffrement — en 1914, 8 commis civils et réservistes, en 1916, 5 officiers, 18 secrétaires d'origines très diverses ;

— 2° Bureau : Cryptographie, comprenant un élément Etudes, avec 3 à 5 officiers et 1 secrétaire et un élément Déchiffrement, avec 7 officiers, 3 secrétaire ;

— 3° « Bureau central de T S F », 1 officier - des secrétaires ;

— 4° Bureau goniométrie : 4 officiers - secrétaires en 1916.

On peut dire qu'à partir de 1916 la section comprenait environ 60 à 70 personnels, dont 25 officiers.

3-312. — La section du Chiffre du G Q G de 7 officiers qui avaient rejoint peu à peu au 13 août 1914 passe à 13 fin septembre et se maintient à ce chiffre qui permet à son chef de disposer de 4 équipes de 3.

Il y avait sans doute aussi quelques interprètes, sous-officiers et dactylos, ce qui fait croire à une effectif d'une vingtaine, dont 12 « producteurs ».

3-313. — Le commandant GIVIERGE réussit assez rapidement à mettre en place un officier spécialisé dans les E-M de chacun des Groupes d'Armes, Armées et C.A. de cavalerie, mais il ne parvint jamais, semble-t-il, à en avoir 2 partout, certains en ayant 3, les autres 1 seul.

3-32. — Comment fut recruté et formé ce personnel ?

Le noyau formé avant guerre fut conservé et les personnels qui avaient dû le quitter ou y avaient été instruits furent rappelés, dans toute la mesure du possible, mais bien des difficultés se présentèrent.

Restaient les nouveaux, à faire affecter et à instruire.

Le commandant CARTIER recruta parmi les personnels des Affaires étrangères mobilisés, tandis que le commandant GIVIERGE réussissait à se faire affecter des officiers de la garde républicaine de Paris.

Ensuite il y eut une cooptation par relations, puis la récupération d'officiers blessés ou inaptes au service du front dont plusieurs se montrèrent inaptes aussi au Chiffre, enfin des affectations prononcées par les directions d'Arme, souvent peu heureuses.

La formation de ces nouveaux chiffreurs fut faite sur le tas à la section du Ministère, tandis qu'au G Q G, le commandant GIVIERGE organisait des stages de 8 ou 15 jours pour les officiers des Armées, essayant de les conserver quelque temps de plus au G Q G pour leur donner un peu de pratique.

Un problème délicat fut posé dès 1915 par les ordres du Ministre et du Commandant en chef fixant une limite aux séjours à l'Intérieur ou dans les états-majors.

L'application d'une telle mesure aurait évidemment détruit le Chiffre français ; aussi ne fut-elle que très partielle et échelonnée. Les meilleurs spécialistes furent conservés, ce qui ne fut pas pour améliorer l'image de marque des chiffreurs aux yeux des combattants !

3-33. — On ne peut finir ce chapitre sans donner les noms des principaux artisans du Chiffre et du Décryptement français pendant la grande guerre. Notre liste sera certes très incomplète, mais on peut citer à la Section du Chiffre du Ministère,

à côté de son chef CARTIER, le capitaine de frégate de MANDAT-GRANCEY, chef du bureau central de T S F, les décrypteurs OLIVARI, PAULIER, LATREILLE, FREYSS, DEJARDIN, SCHWAB, et surtout PAINVIN, qui obtint les plus beaux résultats.

Au G.Q.G., le commandant GIVIERGE appréciait particulièrement le capitaine SOUDART qui fut en quelque sorte son adjoint et le remplaça après son départ.

Enfin on ne passera pas sous silence le lieutenant-colonel THEVENIN qui n'était plus au Chiffre, mais travailla avec succès au décryptement de procédés allemands de campagne.

3-4. — TRANSMISSIONS ET CHIFFRE.

Ce qui n'était encore que la Télégraphie et la Radiotélégraphie militaires œuvrait déjà en étroite liaison avec le Chiffre, tant pour l'acheminement des messages que pour la livraison des messages interceptés, la gonio, etc...

En outre à l'échelon central, la liaison était encore plus étroite, par l'existence du bureau central de T S F au sein de la section Chiffre. Cette union fut souvent très difficile, l'aspect technique cherchant parfois à prendre le pas sur l'emploi ; l'employeur ne comprenait pas toujours les servitudes techniques, ni les difficultés d'une technique naissante ; l'incompatibilité d'humeur apparut aussi entre certains protagonistes et enfin l'arbitre qu'était le Commandement mécontentait l'un ou l'autre ou les deux partenaires, faute de saisir les soucis des deux partis et de bien comprendre les données du problème.

A l'échelon central même, on ne savait pas initialement qui fixerait les missions de la « T.S.F. ». La situation fut souvent tendue entre CARTIER et FERRIE, mais la diplomatie du premier (qui ne faisait que peu confidence de ses difficultés) semble avoir réussi dans l'ensemble à conserver des relations efficaces. Par contre, au G.Q.G., le « torchon brûla » souvent entre GIVIERGE et le lieutenant-colonel puis colonel SIMON, les officiers des 2° et 3° bureaux versant parfois innocemment ou par incompréhension de l'huile sur le feu. Ce phénomène mérite d'être approfondi, car ses divers aspects n'ont pas varié.

Le Chiffre revendiquait en effet :

— la réception directe et intégrale des P.V. et messages interceptés, de façon à pouvoir les exploiter sans retard,

— la possibilité d'indiquer (au besoin directement aux chefs de station) les émissions à écouter et à goniométrer,

— la possibilité d'adresser des observations et de recevoir des informations directement des stations d'écoute et de goniométrie,

— une participation aux décisions d'implantation des stations d'écoute et de goniométrie.

Enfin il se plaignait de nombreuses fautes dans la transmission des messages et du brouillage des stations d'écoute par des réglages ou bavardages intempestifs des stations d'émission.

Le directeur de la Radiotélégraphie militaire voulait être le maître chez lui et n'admettait pas qu'un organisme extérieur donnât directement à ses subordonnés des instructions dont il était averti après coup par ceux-ci. Il voulait aussi contrôler le travail de ses stations et l'organiser à sa guise en fonction des possibilités et résultats techniques. L'Etat-Major était l'intéressé final, tant pour l'acheminement rapide de ses messages que pour l'obtention accélérée des résultats des écoutes, mais l'affaire se compliquait pour trois raisons :

— les écoutes fournissaient des messages clairs et des chiffrés ;

— la Radiotélégraphie militaire pouvait adresser directement la localisation de stations radios et d'états-majors dont les adresses étaient en clair ou qu'elle reconnaissait à ses caractéristiques d'émission ou de manipulation ;

— la Radiotélégraphie militaire était liée au 3° bureau et au 1° bureau (qui avait aussi au début de la guerre les attributions logistiques pour lesquelles on créa ensuite le 4°), alors que les renseignements étaient du domaine du 2°, qui luttait avec raison pour que tous passent par lui alors que le 3° se plaignait des retards de ce filtre.

Le 2° bureau, après s'être désintéressé des écoutes, voulut en reprendre la direction.

Cet ensemble de facteurs contradictoires ne pouvait évidemment que produire des heurts violents, d'autant plus que nos anciens n'avaient pas le caractère facile (confer les querelles des généraux !), malgré le souci chez tous de fournir le service le plus efficace.

Aussi pendant les années 1914 et 1915 les blocages furent fréquents, le « fournisseur » des écoutes parfois excédé par des intrusions dans son domaine prenant des mesures de « rétorsion » et ne voulant plus connaître la section du Chiffre, et envoyant sa pâture à l'état-major où le 2° bureau l'arrachait au 3°.

Enfin après bien des démêlés et des vicissitudes, parut, le 30 juin 1915, une note du 3° bureau relative à l'organisation des écoutes et de la goniométrie qui désignait le 2° bureau comme « employeur ». Comme le Chiffre était rattaché au 2° bureau, un modus vivendi s'établit, peu à peu, qui n'éliminait pas certains heurts qui eurent encore lieu, mais permit une exploitation moins dépendante de la bonne volonté des personnes. Chacun avait eu en outre à faire son apprentissage dans un système nouveau et l'accoutumance des uns et des autres permit des circuits courts facilitant le travail sans empiéter sur les prérogatives des chefs.

Ce problème particulier des écoutes et de la radiogoniométrie a paru intéressant à développer, car il est un des aspects des problèmes Etat-Major - Transmissions qui ont toujours existé, existent encore et ne se règlent que par un état d'esprit coopératif des intéressés, admettant des circuits courts dans les domaines du commandemen technique, de l'exploitation technique comme de l'emploi.

Ces errements eurent d'ailleurs besoin d'être précisés et confirmés. On peut citer à ce propos une note 6385 du G.Q.G. en date du 6 mars 1918 et une autre du 6 mai 1919.

3-5. — COURRIER ET CHIFFRE.

Un autre problème se posa assez rapidement, celui de l'acheminement dans l'état-major des correspondances à chiffrer, chiffrées et déchiffrées.

Tant que le chiffre demeurait l'apanage du chef et de son entourage immédiat (son cabinet), le problème ne se posait pas. Quand le volume et la nature des communications secrètes se développèrent, en même temps que le nombre des « rédacteurs » et des « destinataires », il se posa à la fois un problème de régulation (au sens moderne des Transmissions) et de sécurité.

Au début de la guerre, dans de nombreux états-majors, le Chiffre était partie intégrante du courrier : les correspondances à chiffrer ou déchiffrer y circulaient à nu, les opérations de chiffrement ou de déchirement avaient lieu n'importe où, les textes clairs ne recevaient pas une protection suffisante, d'autant plus que leur diffusion s'accrut rapidement.

La capture d'archives et de documents divers chez l'adversaire après la Marne permit de constater l'intérêt de ces matériaux pour les décrypteurs ; aussi des instructions furent-elles données rapidement pour éliminer ces très graves risques, les documents

clairs durent circuler sous enveloppe et être conservés avec précautions.

Mais de nombreuses questions se posaient :

Les correspondances chiffrées doivent-elles transiter par le bureau du courrier ou circuler directement entre Chiffre et moeyns de transmission ? Les correspondances à chiffrer doivent-elles transiter par le bureau du courrier ou être adressées directement par l'autorité origine au Chiffre. Les correspondances déchiffrées doivent-elles transiter par le bureau du courrier ou être adressées directement par le Chiffre aux autorités destinataires ?

Un problème analogue se posera en 1951 quand l'exploitation du Chiffre sera incluse dans les centres de transmissions, pour le passage des messages à chiffrer ou déchiffrer par la régulation.

Des solutions diverses furent appliquées dans les états-majors, jusqu'au 9 février 1915 où pour le G.Q.G. une note répondit affirmativement à ces trois questions, rendant les passages par le courrier obligatoires, à chaque mouvement.

Le Chiffre du G.Q.G. respecta évidemment cet ordre quoique ses préférences eussent été d'adresser directement les messages déchiffrés aux destinataires, pour des raisons de rapidité et de sécurité ; ce point de vue motivé restera d'ailleurs toujours celui du Chiffre, alors que le courrier et régulation s'y opposeront toujours, également avec raison, pour pouvoir suivre les documents de bout en bout et faciliter les recherches.

Mais cette note n'avait pas réglé tous les problèmes, ceux des échelons subordonnés en particulier, où la fantaisie régnait, et celui de la diffusion des messages à chiffrer et des messages déchiffrés. Cette diffusion beaucoup trop étendue et sans démarquage faisait en effet courir des risques graves.

Le 17 décembre 1915, une Instruction provisoire sur l'organisation du service de la correspondance chiffrée donnait tous les ordres nécessaires, mais son application fut loin d'être immédiate dans les Etats-Majors de groupes d'Armée et d'Armées auprès desquelles de nombreuses démarches durent être faites. Aux échelons plus petits et dans les régions militaires, il semble que le système « chiffre de cabinet » resta en vigueur.

3-6. — DIRECTION DU CHIFFRE.

3-61. — Chiffres.

L'Armée française commençait la guerre avec des dictionnaires codiques modèle 1912 et le procédé S D 12, ainsi qu'avec un dictionnaire franco-anglais et un dictionnaire franco-russe.

Il paraît utile de rappeler, pour information, le voyage du Président POINCARE en Russie juste avant les hostilités.

Dans leurs déplacements, Président et Ministres employaient alors un dictionnaire du commerce (NILAC) sans surchiffrement. Pour ce voyage en Russie, et compte tenu des circonstances, la section du Chiffre obtint que les télégrammes soient surchiffrés, par le système S D 12, avec emploi d'une clé différente pour chacun (clés-une-fois).

Les périodes de la mobilisation et de la retraite sur la Marne, suivies du séjour de la section du Chiffre à Bordeaux (début septembre 1914 au 6 ou 8 janvier 1915) ne se déroulèrent pas sans difficultés.

On ne sut pas d'abord si les corps d'armée envoyés en couverture avaient emporté leurs dictionnaires et lesquels (Paix ou Guerre) aussi décida-t-on d'employer le procédé S D jusqu'à nouvel ordre.

En outre on prescrit le retrait des dictionnaires des corps de cavalerie, en raison du risque de capture par l'ennemi.

On s'aperçoit très vite que le S D est mal employé et les clés sont changées plus rapidement que prévu (21 août, 25 août, 1er, 7, 17 et 30 septembre). En outre l'ennemi a capturé des notices du procédé, aussi crée-t-on une variante (modification du nombre des diagonales) pour les hautes autorités (jusqu'à l'Armée).

La T.S.F. pose aussi très vite des problèmes. L'écoute des postes allemands montre les renseignements que l'on peut tirer d'indicatifs invariables et des messages de service (ou bavardages) entre opérateurs. Aussi, le 12 ou 13 août, décide-t-on une variation quotidienne des indicatifs au moyen de tableaux fournis par la section du Chiffre et on crée un code de service T.S.F., car le S.D. prévu jusqu'alors était trop difficile et trop lent.

Pour les places fortes on avait aussi en août décidé d'améliorer la sécurité de leur chiffre : code paix plus transposition fixe dans chaque groupe.

En octobre, un nouveau dictionnaire « rouge » est mis en service pour les grandes unités.

Fin 1914 on remet en service un code aéronautique 1912, après quelques recherches dues à la dispersion, avec un surchiffrement par transposition dans chaque groupe. On remit aussi en service des dictionnaires anciens, pour des besoins spéciaux.

On décide aussi de changer les clés S D régulièrement toutes les semaines.

Une certaine routine s'installe, coupée seulement par des incidents qui obligent à modifier la cadence des changements de dictionnaires ou de clés et l'établissement de nouvelles liaisons.

On relève la création de nouveaux dictionnaires spéciaux :

— Mai 1915 :
  — pour les hauts niveaux (jusqu'à groupe d'Armée),
  — pour les relations avec les missions à l'étranger ou auprès des armées étrangères ;
— en octobre -915 : pour les attachés militaire ;
— début 1916 : pour les services de ravitaillement (service des arrières).

Les dictionnaires courants (Armée - C.A. - Div) semblent changer à peu près tous les ans. En outre des suppléments géographiques sont édités ou complétés régulièrement. Mais la section du Chiffre du Ministère, comme celle du G.Q.G., savent parfaitement qu'un dictionnaire surtout ordonné n'apporte qu'une sûreté très limitée dans le temps, même avec les changements de pagination usuels. Aussi décide-t-on peu à peu l'emploi de procédés de surchiffrement.

Le 30-9-1915, le Ministre décide le surchiffrement par le procédé S D des télégrammes importants (jugés tels par l'expéditeur).

Le 24-12-1915, le G.Q.G. décide de surchiffrer tous les télégrammes chiffrés par dictionnaire dans les Armées. Le procédé est une transposition dans chaque groupe, donc assez simple, et faible.

Le 22-8-1916, le G.Q.G. décide d'adopter un procédé de surchiffrement voisin du S D (transposition avec I diagonale, 2 clés mensuelles) sur tous les télégrammes chiffrés par dictionnaire.

Le procédé sera peu après adopté par le Ministre et généralisé.

Parmi les cas particuliers on peut citer :

— la mission du général JANIN en Russie en 1916 est dotée de 2 systèmes particuliers : une clé personnelle pour le général (sur dictionnaire) et pour sa mission, une substitution à deux alphabets incohérents, dont l'alternance est donnée par un livre (clé indéfinie une fois) :

— la mission du général BERTHELOT (en Orient ?) emploiera un surchiffrement lettres-chiffres (tableau carré de 25 lettres, 2 chiffres correspondant à chaque ligne ou colonne) ; il devait donc être doté d'un dictionnaire littéral, alors que tous les dictionnaires militaires français connus de cette époque sont en chiffre ;

— le problème de l'Armée d'Orient : l'Armée d'Orient relève du G.Q.G. jusqu'au départ du général JOFFRE, du Ministre ensuite ; elle pose des problèmes particuliers parce qu'elle est loin et parce qu'elle comprend des unités étrangères. Initialement elle n'avait pas d'officier du Chiffre, mais on s'aperçoit vite que non seulement elle en a besoin, mais aussi d'une petite section Chiffre, mise en place avec difficulté, compte tenu des rapports entre le G.Q.G. et l'entourage du général SARRAIL qui y voyait des « mouchards » du G.Q.G.

Elle a donc besoin d'un chiffre spécial avec la France (code diplomatique plus clé de surchiffrement), de moyens lui permettant d'être en liaison avec certaines missions à l'étranger (Roumanie - Russie), d'un ensemble interne qui comprendra : le chiffre de l'armée française subordonnée, le chiffre avec les armées étrangères ou plutôt avec les officiers de liaison auprès de ces armées, auxquels on donnera un dictionnaire particulier avec un système de surchiffrement spécial, différent de la transposition employée dans les armées françaises, enfin un Chiffre pour l'Armée serbe.

Parmi les incidents marquants on peut citer :

— des erreurs de non-spécialistes du chiffre, dans les régions militaires ou les missions à l'étrenger ; des mélanges de clair et de chiffré (par dictionnaire) ce qui impliqua des rappels à l'ordre brutaux ;

— des renseignements envoyés en Chiffre par la voie militaire et en clair par la voie civile (Intérieur) sur l'effet des bombardements allemands sur les arrières ou à l'intérieur ;

— le code T.S.F. employé pour autre chose que le service T.S.F., en particulier pour certaines informations tactiques.

On peut résumer tout ce qui précède en disant que :

— l'Armée française, partie en guerre avec un petit nombre de dictionnaires utilisés à nu et un procédé littéral à transposition, l'a terminée avec un plus grand nombre de dictionnaires, certains spécialisés, tous utilisés avec un surchiffrement par transposition solide (clés en général mensuelles), et le même procédé littéral devenu en fait moyen de secours car peu utilisé, et rendu sûr par le changement hebdomadaire des clés.

— on peut noter aussi que les réseaux initialement très étendus (en fait à toute l'Armée) se sont cloisonnés ;

— compte tenu des moyens de décryptement de l'époque, on pouvait estimer qu'avec la mise en œuvre généralisée du surchiffrement en 1916, ces systèmes donnaient la sûreté recherchée ; aucune preuve contraire n'a été donnée.

3-62. — Camouflage (ou chiffrement de l'Avant).

Le premier titre de ce paragraphe est un anachronisme car ce n'est en fait qu'en 1939-1945 et surtout ultérieurement qu'une distinction nette s'est établie entre le Chiffre et les procédés de sûreté très limitée destinés aux petites unités, auxquels a été donnée cette dénomination, mais elle a été adoptée ici, pour ne pas créer de confusion dans l'esprit des lecteurs actuels.

Dès consolidations de la guerre de position et en raison de l'augmentation du trafic, on réclame un moyen de chiffrement simple et rapide pour les divisions et brigades : les inventeurs ne manquent pas, qui proposent le bon vieux Jules CESAR ou des systèmes qui se résolvent en fait à des substitutions simples à représentation unique, qu'elles soient manuelles ou pseudo-mécanisées (cadrans ou réglettes genre St-Cyr). Fleurissent aussi les mots conventionnels, évidemment invariables. Tout cela n'est pas grave tant que la communication se limite au port de plis, mais devient crucial lorsque le développement de la T.S.F. et du téléphone puis de la télégraphie par le sol (T.P.S.) atteint l'avant, car l'adversaire, comme les Français, est en mesure d'intercepter et ne s'en fait pas faute.

Le caractère critique de ce problème est signalé officiellement par le général DUBAIL au début de 1916, pour le téléphone : il indique que les Allemands camouflent leurs communications et propose l'emploi d'un système à cadran (2 alphabets ordonnés décalés, dont la position relative changerait à chaque message. La section du Chiffre du Ministère propose un système bifide à représentation multiple (tableau carré à 25, 36 ou 100 cases avec 2 ou 3 signes pour chaque ligne ou colonne). La section du Chiffre de G.Q.G. repousse le système à cadran (Jules CESAR) et propose soit un système S D simplifié (sans doute sans diagonale) avec feuilles de clés matriculées, soit le tableau littéral de 25.

Des essais sont faits à la 2e Armée : l'appareil à cadran avec alphabets incohérents et le système de la section du Ministère, c'est-à-dire le système à 25 cases avec un fascicule de 6 tableaux, plus un codage pour les chiffres et les mots usuels.

Tout cela paraît insuffisamment sûr ou trop compliqué et le 22 mars 1916 le G.Q.G. décide l'emploi de carnets de camouflage téléphonique. Les carnets sont en fait de petits codes en 3 chiffres (comme il en existe encore) ils comprennent 300 mots. L'emploi d'une clé additive est prévu mais non obligatoire.

Malgré certaines craintes, ces carnets sont accueillis favorablement par les échelons inférieurs (régiment - groupe).

On prévoit de les changer tous les quinze jours, ce que d'aucuns (section du Chiffre du Ministère) trouvent insuffisant, avec un cloisonnement créant une dizaine de secteurs sur le front.

Le besoin serait de 4 000 carnets par mois ; leur impression coûterait 1 000 francs (or), ce qui fait beaucoup hésiter le G.Q.G. et le Ministère ! A la même époque la 2° Armée qui se manifestait beaucoup depuis un an par des erreurs et maladresses de chiffrement soulève le problème de la T.S.F. de l'avant jusqu'à division) et propose un système simple et ridicule (GIVIERGE) ; à cette même Armée les radiotélégraphistes employaient alors de leur propre chef des procédés fantaisistes dénués de toute sûreté. Le G.Q.G. réagit en interdisant les procédés non réglementaires et en prescrivant l'emploi du S D agrémenté de groupes conventionnels pour raccourcir les messages (mais tous terminés par X ce qui paraît un non-sens, à la réflexion) jusqu'à l'échelon division et les carnets susvisés au-dessus.

En fait le véritable chiffre sera maintenu pour les communications télégraphiques et radiotélégraphiques (à partir de l'échelon division) et les carnets utilisés pour les conversations téléphoniques (1) et les communications de T.P.S. et de T.S.F. à l'intérieur des divisions. Il y eut tout de même des réticences à l'emploi des carnets, surtout à la 2° Armée, qui tenait à ses dangereux errements et ailleurs où l'on avait pris l'habitude de mots conventionnels invariables.

Mais le Commandant GIVIERGE obtient que les officiers du Chiffre des Armées soient autorisés à prendre le bâton de pélerin pour semer la bonne parole dans les divisions (et les contrôler), ce qui n'avait jamais pu se faire auparavant et la situation s'améliore.

Il avait été décidé en juin 1916 d'avoir un carnet par Armée et, pour faire des économies (!), de réutiliser de temps à autre d'anciens carnets. On s'aperçoit que les relèves des divisions

(1) Compte tenu de son expérience, le rédacteur doute que les colonels et généraux les aient effectivement utilisés !

produisent quelques désordres, que certains ont été pris par l'ennemi et que des mots conventionnels sont toujours utilisés par nous (comme par les Allemands d'ailleurs).

Le problème du camouflage demeurera tel jusqu'à la fin de la guerre (1).

3-63. — Acheminement et Procédures.

Ce chapitre ne peut se clore sans souligner deux points qui soulèvent toujours des difficultés, les marquants de systèmes et les adresses. Un autre point, également permanent, ne fut qu'abordé à l'époque, celui des marquants de clé, car la clé était la même pour tous les usagers d'un système pendant la cryptopériode considérée, ou, pour les systèmes particuliers où elle changeait, était indiquée par un groupe convenu particulier, parfois répété en fin de message et constituant en même temps le marquant de système ; certains étaient très compliqués et comportaient jusqu'à 3 groupes de 5 chiffres.

Le nombre de réseaux était faible et on se contenta de placer en tête du cryptogramme (comme dans la plupart des pays d'ailleurs) un groupe codique invariable, qui était constitué d'un même chiffre répété 5 fois : exemple 00000, 22222, etc..., et on parlait du code ou du réseau 00 ou 22.

En fait il ne semble pas qu'on se soit jamais préoccupé de dissimuler à l'adversaire, ni en France ni à l'étranger, le réseau ou le système auquel appartenait un message, quoique cela facilite le travail des cryptologues et même la reconstitution de l'ordre hiérarchique quand il y a cloisonnement (ce qui n'était pas le cas général d'ailleurs).

Le problème du codage des adresses n'apparut à l'origine ni chez les Allemands ni chez les Français. En télégraphie filaire, on employait l'adresse en clair avec même l'indication du lieu de stationnement. En radiotélégraphie, initialement, l'indicatif radio tenait lieu d'adresse et si le destinataire était une autorité voisine ou autre sa désignation figurait dans le texte chiffré. Il a été indiqué plus haut que dès août 1914 il avait été décidé en France de changer quotidiennement ces indicatfs, mais il n'est pas certain que cette mesure ait été appliquée sur les grandes

(1) On peut même dire qu'il n'est pas résolu à l'heure actuelle et ne le sera jamais en raison de l'antinomie vitesse-secret et du désir excessif de simplification des exécutants, au moins en France.

liaisons (Paris-Petrograd ou Paris-Salonique par exemple), d'autant plus que certains postes radios, comme la Tour Eiffel, étaient particulièrement reconnaissables par leur puissance ou leur note.

La question se posa aussi des adresses multiples, pour la diffusion des messages à plusieurs destinataires ; il semble qu'on ait employé des groupes codiques invariables en tête du texte des messages comme JOGAL qui indiquait que les messages reçus à Chantilly par le G.Q.G. devaient être retransmis sans délai au Ministère et à diverses autorités parisiennes.

3-7. — EXPLOITATION.

L'exploitation du chiffre demeure le monopole des officiers (et des commis ou civils assimilés, au Ministère) mais, comme nous l'avons dit plus haut, le travail n'est le fait de spécialistes qu'à l'Administration Centrale et au G.Q.G.

Aux Armées, seuls les Groupes d'Armées et Armées disposent d'un, deux ou trois spécialistes suivant les possibilités ou l'humeur du chef d'état-major, le reste des chiffreurs - déchiffreurs nécessaires pour le travail d'exécution est formé de suppléants, d'officiers d'état-major (en général du 2° bureau) sur lesquels tombe la corvée.

On ne peut donc s'attendre à un bon travail, surtout lorsque le volume du trafic s'accroit.

On ne peut établir de statistiques, faute d'information ; le commandant GIVIERGE nous fournit pourtant quelques chiffres parlants :

— en avril 1916, soit en moins de 2 ans, la mission française auprès de la STAVKA (G.Q.G. russe) avait reçu 1071 télégrammes chiffrés et émis 1580 ;

— en juillet 1915, le G.Q.G. reçoit et émet 2500 télégrammes chiffrés (60 à 120 par jour) ;

— en août 1916, il y a plus de 40 télégrammes reçus de l'étranger par jour, représentant plus de 8 000 groupes (200 groupes par message) pleins de fautes en raison des mauvaises transmissions.

Et cela sans compter le déchiffrement des télégrammes allemands interceptés qui à cette époque montait à plus de 40 par jour.

Ces chiffres ne sont pas très élevés, et correspondent par mois au trafic journalier d'un état-major actuel, mais il faut penser que la brigade était de 3 officiers, que le travail était entière-

ment manuel et que certains messages demandaient plusieurs heures de travail du fait des erreurs de transmission ou de chiffrement dont ils fourmillaient.

On peut dire qu'en règle générale les chiffreurs ne chômaient pas et n'avaient pas le temps, au désespoir de certains d'entre eux, de faire des recherches de décryptement. On relève en effet sans cesse des plaintes contre les Transmissions et les chiffreurs occasionnels.

Des incidents avec les transmissions (P.T.T. ou militaires) sont dus au nombre de groupes, problème qui se reposera plus tard, le chiffre n'incluant pas les groupes clés dans son dénombrement et inversement ce qui amène des erreurs avant qu'on se soit mis d'accord. Les P.T.T., à un moment, groupent les messages en tranches de 50 et l'on ne sait plus comment les rabouter car les parties ont été mélangées aux relais.

Pertes de documents, emploi de clés périmées, mélange de clair et de chiffré, groupes ou lettres sautés (ce qui est grave dans le S D) ; inobservance du démarquage technique, telles sont les critiques habituelles à l'égard des chiffreurs occasionnels. Le Commandement réagit périodiquement en rappelant la nécessité de conserver le secret, de désigner du personnel apte et en organisant des exercices : exemple d'une circulaire du 22 janvier 1915 signée par le major général (général PELLE) prescrivant un exercice de chiffrement ou déchiffrement quotidien (à cette époque le trafic était très faible).

3-8. — DECRYPTEMENT ET DECHIFFREMENTS.

3-81. — Le travail effectué avant 1914 a permis d'avoir quelques idées sur les chiffres étrangers, quelques décryptements et déchiffrement de systèmes basés sur des dictionnaires, et la reconnaissance d'un procédé allemand appelé Uebchi.

C'est sur ce système qui continue à être employé au début de la guerre entre grandes unités que va s'exercer l'effort principal.

Cependant le Chiffre, chargé initialement (surtout par lui-même), faute d'ordre et d'organisation en la matière, de toute l'exploitation des écoutes, remplira efficacement cette mission, jusqu'à ce qu'il passe la main au 2° bureau pour l'analyse des réseaux et l'exploitation du clair (décision du 30 juin 1915).

Dès le 10-11 août, il est possible d'indiquer la correspondance entre indicatifs et états-majors, et le 12, grâce aux indications fournies par les diverses stations d'écoute sur les niveaux de

réception, on peut donner une idée assez précise de la concentration allemande ce qu'apprécie fort le général BERTHELOT. De même au début de Septembre, le commandant CARTIER peut signaler, avec un jour d'avance sur l'aviation le glissement vers le Sud-Est des Armées Von Klück et Von Bülow qui permettra la victoire de la Marne.

Ensuite, régulièrement, avec l'aide des opérateurs radio qui identifient les opérateurs adverses, et ultérieurement par la goniométrie, on pourra établir sans retard la correspondance indicatifs-grandes unités et localiser de façon de plus en plus précise les grandes unités desservies par des postes radios actifs.

Cette connaissance de l'origine des messages, les messages de service échangés entre opérateurs, les répétitions de messages chiffrés ou de parties de ceux-ci, les répétitions des mêmes messages rechiffrés avec le même code ou avec des codes différents donneront des éléments très utiles et même parfois déterminants pour décrypter les messages chiffrés interceptés.

3-82. — Chiffres tactiques allemands.

C'est donc à Uebchi (1) que s'attaquent dès l'abord tous les décrypteurs, autour de CARTIER et de GIVIERGE. On sait qu'il s'agit d'une transposition double, avec une seule clé et des lettres nulles (X) placées suivant une loi inconnue.

L'étude initiale est rendue très difficile par les fautes de transmission, aussi bien allemandes que françaises.

Enfin le 20 septembre la section du Chiffre reçoit une instruction allemande sur le Chiffrement et le Déchiffrement et le 29 septembre une première clé est trouvée, grâce à 3 télégrammes de même longueur. Mais la clé change tous les 5 ou 6 jours.

Une seconde clé est trouvée au début d'octobre au bout de 19 heures de travail et dès lors, la méthode étant au point, il ne faut pas plus de quelques heures à chaque changement. Ces clés sont communiqués à la section G.Q.G.

Mais une indiscrétion est commise : le journal Le Matin, sans doute par suite d'un bavardage dans l'entourage du Président

---

(1) Les Allemands appelaient ce système Doppelwürfel : double racine ou double clé !

Les Français l'appelaient Uebungschi, parce qu'avant guerre, le système était utilisé pour des messages d'exercice commançant par Uebung.

POINCARE, indique que c'est par le déchiffrement d'un télégramme allemand que les Français ont su que GUILLAUME II se rendait à THIELT où des avions français sont allés bombarder.

Le 28 novembre on constate un changement du système allemand, quelques Uebchi subsistant encore pendant près d'un mois.

On reconnaît assez vite, qu'il s'agit d'une substitution Jules CESAR à 3 alphabets successifs répétés, suivie d'une transposition.

Le 10 décembre, le lieutenant-colonel THEVENIN trouve : ABC + transposition à 15 colonnes puis une autre clé à 25 colonnes peu après. Après bien des tâtonnements, une méthode générale assez simple est mise au point et appliquée.

En janvier-février 1915, le trafic radio allemand est faible et les écoutes mauvaises, les clés ne peuvent être envoyées au G.Q.G qu'au bout de 8 à 15 jours, mais ensuite, la méthode s'affirmant et l'expérience aidant, 48 heures suffiront en général.

Sur le front russe le trafic est beaucoup plus important, notre mission à la STAVKA (G.Q.G. russe) envoie le trafic intercepté à Paris qui trouve des substitutions simples et le système ABC et envoie les clés. En octobre 1915, on retrouve encore quelques Uebchi, dont le décryptement continue.

En janvier 1916 apparaît un nouveau système du même genre, avec 4 Jules CESAR successifs ABCD suivi d'une transposition simple, mais la séquence ABCD ABCD A... est rompue suivant une loi inconnue, qui est trouvée le 5 février par les anglais du Q.G. britannique en France (une bonne liaison existait entre eux et le G.Q.G. et ils recevaient tous les éléments découverts par les sections du Ministère et du G.Q.G.) : elle découlait de la clé de transposition.

Le 6 mars PAINVIN trouve la nouvelle clé en service, mais on s'aperçoit aleors que les messages échangés sont en fait des messages d'exercice et qu'il n'y a plus d'envoi de messages réels par radio.

Le 20 mars le système ABCD disparaît à l'Ouest, alors que l'A.B.C. demeure en service sur le front russe.

Sur le front français apparaissent alors de nombreux systèmes (un par Armée) qui donnent de la tablature à nos décrypteurs, non par leur difficulté, mais par leur nombre qui surcharge la petite équipe de la section du Ministère.

On reconnaît notamment :

— une substitution à double clé à partir d'un tableau carré, on avance d'abord d'une colonne à chaque heure, puis à chaque groupe du message ;

Il y a 4 alphabets incohérents, ce qui donne 4 tableaux distincts, indiqués par un marquant ;

— une substitution simple, par cadran sans variation ;

— du Jules CESAR ou équivalent dans le Nord ;

— des substitutions simples en lettres ou chiffres, avec emploi de petits codes en 2 lettres.

La substitution à double clé à un seul tableau semble se généraliser, le marquant de système étant un bigramme répété, avec séparation par une lettre nulle ; le même tableau est utilisé pendant 3 semaines.

PAINVIN rétablit pratiquement toutes les clés, sans retard excessif pour l'exploitation des messages (2 à 5 jours).

Le 28 septembre apparaissent de nouveaux systèmes :

— lettres représenttes par un ou deux chiffres (substitution simple),

— substitution à double clé, à alphabet décalé, la première lettre du cryptogramme donnant la lettre initiale de cet alphabet, avec changement de colonne à chaque groupe,

— substitution à double clé où la permutation des lettres dans les alphabets successifs se fait par demi-colonne etc...

Tous ces systèmes ne tinrent pas non plus au-delà des quelques jours indiqués plus haut, parce qu'on relevait des parties communes dans les télégrammes (recouvrements) et que les changements de colonne étaient réguliers et insuffisamment fréquents.

En octobre 1916, le G.Q.G. déchiffrait plus des 3/4 des messages interceptés (40 à 45 par jour).

Les interceptions téléphoniques du champ de bataille font apparaître l'emploi très large de mots conventionnels (qui ne changent pas) de petits codes (CHIFFRIERTAFEL trouvé par la 10° Armée) de carnets de chiffrement du même type (carnet de chiffre par téléphone N° 107 perdu par la 45° Ersatz division) etc...

Puis en mars 1918 tous ces systèmes disparaissent et les télégrammes interceptés ne sont que des suites incohérentes des 5 lettres ADFGX ; l'analyse des fréquences montre qu'une clé doit changer tous les jours. Le nom officiel allemand du système était : Geheimschrif der Funker 18 (en abrégé GEDEFU 18).

En mars, peu de télégrammes sont échangés, la matière de travail manque et le Chiffre français est découragé.

Mais le 1° avril, PAINVIN remarque des messages ayant des parties communes, et le 5 avril la clé est trouvée. Il s'agit d'une substitution des 25 lettres usuelles par les 25 bigrammes formées avec ADFGX, suivie d'une transposition simple.

Les clés sont alors reconstituées dans un délai maximum de 20 jours, la clé du 28 mai étant livrée le 30, celle du 30 le 1° juin.

Le premier juin, les 5 lettres deviennent 6 : ADFGVX ; la clé est trouvée le 2 ; les 36 bigrammes possibles correspondent aux 2 5lettres, aux 10 chiffres et au point, ce qui avait l'avantage de réduire la longueur des messages.

Rien de nouveau jusqu'à l'Armistice, mais on ne saurait terminer ce paragraphe sans parler du « Télégramme de la Victoire ».

La clé trouvée le 2 juin permet en effet de déchiffrer le soir même le texte : « Hâtez ravitaillement en munitions. En terrain couvert également pendant le jour ». Les services de goniométrie confirment l'expéditeur (G.Q.G. allemand) et le destinataire (E.M. d'Armée entre Mont-Didier et Noyon). L'Etat-Major français connaît ainsi l'axe de la prochaine attaque allemande qui échouera grâce à une contre attaque du général MANGIN, alors que la situation des alliés était critique.

3-83. — Autres chiffres allemands.

3-831. — Les autres systèmes de chiffrement allemands, utilisés principalement pour les liaisons avec les ambassades, les attachés militaires en mission à l'étranger et la Marine sont tous apparus comme des codes employés initialement sans surchiffrement, puis avec des surchiffrements simples.

Il semble qu'ils aient été tous percés à jour assez rapidement dès que les matériaux (volume de télégrammes) nécessaires eurent été obtenus, en partie parce que les dictionnaires utilisés étaient proches les uns des autres (vocabulaire) et généralement ordonnés.

La condition essentielle du succès fut donc de rassembler un nombre important de cryptogrammes ce qui, initialement, fut difficile, car le moyen quasi-unique était l'interception radio, dont la qualité et le développement furent assez longs à obtenir. En outre, et pour les mêmes raisons techniques, le trafic radio

allemand fut assez faible au début de la guerre. Cependant il n'y eut plus de difficultés de ce côté à partir du deuxième semestre 1915.

3-382. — Les deux premiers systèmes qui peuvent être attaqués furent le KAV et le HAVAUBE, ainsi dénommés à cause de leurs marquants.

Le KAV se présentait sous forme de groupes de 3 lettres et de 5 chiffres, que l'on commence à étudier fin 1914. On reconnaît assez vite qu'il s'agit principalement d'informations météorologiques à l'usage de la Marine. En juin 1915, une centaine de mots du code à 3 lettres avaient été rétablis et on rétablit ensuite peu à peu ce code ordonné. On constate aussi que les noms de bateaux sont camouflés par substitution simple et qu'éventuellement le texte littéral est affecté d'une substitution simple indiquée par un marquant particulier. Fin 1915, le code était quasi intégralement rétabli et le déchiffrement des messages se faisait sans difficulté. On apprit fin 1916 que les Anglais avaient le code depuis le début de la guerre, car il avait été récupéré par les Russes sur une des victimes du naufrage du croiseur MAGDEBURG et transmis par ceux-ci aux Anglais.

Le code HAVAUBE était en groupes de quatre lettres ; on arrive à rétablir certains groupes dès la fin de 1914 et en octobre 1915, les traductions se font sans difficultés, la section du Chiffre et le commandant GIVIERGE ayant rétabli de proche en proche un grand nombre de groupes. Ce travail fut facilité parce qu'on s'aperçoit assez vite que ce code était voisin du code 604 dont on avait pu se procurer une photographie par des moyens illicites peu avant la guerre.

Ce code HAVAUBE était employé aussi pour les liaisons avec les ZEPPELINS. Fin 1915, un surchiffrement de ce code apparaît, il consiste en une substitution simple sur deux lettres des groupes de 4, son emploi était indiqué par le marquant NORD.

Un télégramme particulièrement intéressant fut déchiffré au début de 1916, il indiquait les heures d'ouverture des filets anti-sous-marins du Grand Belt. Il fut communiqué aux Anglais et facilita largement l'action des sous-marins anglais en Baltique. D'ailleurs les Anglais étaient tenus au courant au jour le jour de nos progrès dans la connaissance de ce système.

Le HAVAUBE dont les Allemands pensaient qu'il pouvait être compromis à la suite de la chute d'un ZEPPELIN (nous avions en effet récupéré un code à demi-brûlé, inutile puisque nous l'avions déjà rétabli) fut remplacé au printemps 1915 par le

FUNKSPRUCHVERKEHRBUCH. Ce code était plus complet que le précédent, et avait un plus grand nombre de représentations pour les mots fréquents. Il était en 4 lettres mait fut rapidement rétabli.

3-833. — Les liaisons allemandes avec l'Orient trent apparaître de nouveaux codes en 4 et 5 lettres, après quelques systèmes très simples utilisés sans doute pour le service radio. On releva en février 1915 de la transposition simple entre BERLIN et CONSTANTINOPLE, en particulier un message adressé à un Major Schlee puis des groupes de 4 chiffres. Ce fut le code GERMANIA ETAPPEN (en abrégé G.E.), utilisé quelquefois mélangé à du clair, ce qui facilita les entrées.

Le travail de remontée fut fait par GIVIERGE, quand il avait du temps libre, puis par la section du Chiffre, en collaboration avec lui.

Fin 1915, ce code G.E. était à peu près rétabli et les messages traduits. Les travaux continuaient et sur l'ensemble du trafic allemand vers l'extérieur, on reconnaissait 3 familles de codes, basées respectivement sur le GERMANIA ETAPPEN, sur le SATZBUCH (code civil dont la section du Chiffre avait un exemplaire) et sur un code diplomatique en 4 chiffres.

En novembre 1915, les documents interceptés par les stations d'écoute fournissaient au décrypteurs et déchiffreurs plus de 1 500 documents par jour, à étudier et à classer.

On remonta ainsi un code MACKENSEN (du nom du général allemand qui envahit la Roumanie) d'environ 10 000 groupes régulièrement ordonnés, utilisé notamment dans les compte-rendus de fin de journée, en mélangeant clair et chiffré ; un code FALKENHAYN parallèle au précédent, en groupes de 5 chiffres (10 301 à 20 655) et enfin un troisième, utilisé par les attachés militaires allemands à Athènes et à Sofia, fait de groupes de 5 chiffres, ordonné, employé parfois avec une transposition interne à chaque groupe (45 123) et où les chiffres étaient tous représentés par des groupes commençant par 92.

Tous ces codes furent utilisés jusqu'à la fin de la guerre, avec diverses variantes, mais toujours ordonnés, avec seulement des changements de pagination et des surchiffrements par groupes, assez simples pour ne pas poser de problèmes ardus aux décrypteurs.

Un trafic fort intéressant à suivre, pour de multiples raisons, fut celui échangé entre l'Allemagne, son ambassade et ses consuls en Espagne.

L'attaché militaire utilisait un code en cinq chiffres, à nu ou avec un surchiffrement assez simple : transposition sur chaque groupe ou substitution sur le 1°, le 3° et le 5° chiffre.

L'ambassadeur avait un code en 4 chiffres, et les consuls utilisaient un code identique à celui de l'Amirauté, mais avec une clé additive qui changeait rarement.

Nous parvînmes à traduire tous ces messages rapidement et régulièrement ; la preuve en est donnée par l'affaire Matahari, dont un télégramme indiqua le matricule allemand (H 21) et divers détails qui la conduisirent au poteau de Vincennes.

Enfin le travail de la section du Chiffre ne cessa pas avec l'armistice et, pendant la conférence de la Paix, les relations entre l'Allemagne et ses ambassades à l'étranger, Madrid en particulier, fournirent des informations utiles aux dirigeants français.

3-84. — Autres chiffres étrangers.

3-841. — Bulgarie :

Les Bulgares utilisaient en général des codes à 4 chiffres, dont le remontage ne posa pas de grosses difficultés, en particulier on lisait facilement en novembre 1916 le code des attachés militaires (notamment avec Athènes). Une difficulté vient cependant du fait qu'ils employaient un grand nombre de codes, à vrai dire tous parallèles, mais les décalages demandaient un travail assez important.

3-842. — Autriche-Hongrie :

Le Chiffre autrichien était renommé pour son sérieux et son efficacité. Leurs télégrammes chiffrés attirèrent d'autant plus notre attention que les Italiens avaient, dès avant leur entrée en guerre, demandé notre aide.

On constata d'abord l'emploi de nombreux tableaux de substitution à nombreuses colonnes, utilisés en général en substitution à représentation multiples ; il ne semble pas qu'à Paris tout au moins on ait fait un gros effort pour remonter ces systèmes et déchiffrer les messages correspondants : ce travail fut sans doute laissé aux Italiens.

En novembre 1916 on releva l'emploi de codes en 4 ou 5 chiffres, surchiffré par substitutions simples, avec un petit nombre de clés. Il semble que la section du Chiffre de Paris ait remonté du moins partiellement ce code qui avait été employé en particulier par la Marine.

3-843. — Espagne :

La correspondance Espagne-ambassadeur en Allemagne était d'autant plus intéressante que si le roi restait neutre et assez favorable à l'Entente, certains milieux espagnols auxquels appartenait l'ambassadeur étaient des partisans affichés de l'Allemagne. Il semble, d'après certains renseignements, que l'on ait traduit à plusieurs reprises (notamment après l'Armistice) des télégrammes échangés en un code espagnol assez simple, ainsi que des messages entre l'Espagne et le Maroc espagnol, mais aucune information précise n'apparaît dans les documents actuellement disponibles.

3-85. — Sécurité.

L'affaire de Thielt, rappelée ci-dessus (3-72), avait montré le danger de laisser filtrer des informations sur les décryptements que savait faire la section du Chiffre et son souci de sécurité en fut accru.

En fin 1915, il fut décidé d'appliquer une procédure spéciale pour la sécurité des informations provenant de décryptements et de déchiffrement. Les renseignements ainsi obtenus s'appelèrent dorénavant « renseignements spéciaux », les documents correspondants portant cette mention et devant être conservés uniquement par le 2° bureau qui en tenait un registre spécial.

Néanmoins au début de 1916, la presse fit état de la présence d'un sous-marin à Barcelone, alors que ce renseignement provenait d'un déchiffrement.

Des mesures complémentaires de sécurité furent alors prises, notamment au cabinet du Ministre de la guerre et pour la communication de tels renseignements aux membres du gouvernement et à leurs cabinets.

(à suivre)

COMPOSITION ET ACTIVITES DE LA COMMISSION DU CHIFFRE - 1889-1914

Année	Président	Secrétaire	Membres	Décisions ou avènements
1889	Gal de SESMAISONS (sous-chef EMA)	Lt-Cl PHILIPPE (chef section télégraphie EMA)	Cdt JOSSE - Cne MUNIER (EMA) - Cdt STRAFORELLO (CAB).	
1890	Lt-Cl DELANNE (EMA)	Cdt JOSSE (EMA)	Cdt BERTHAUT (S. géog.) - Cdt BRUN - Cne MUNIER (EMA) - Cdt STRAFORELLO (CAB).	DICT 1890 type 1 (Paix) type 2 (Guerre)
1894	Gal MOUTZ (Insp. T.M.)	Lt-Cl BERTHAUT (Sce Géog.)	Lt-Cl BRUN (ESG) - Cdt JOSSE - Cdt PICQUART - Cne TASSIN (EMA) - Cne LEGRAND (CAB).	Cherche chiffre 2° degré repousse deux systèmes, du Cdt MUNIER et du Cne VALERIO.
1895	Gal LEPLUS (Insp. T.M.)	— d° ? —	d° - moins Cne TASSIN et Cne LEGRAND — plus Cne de ROZIERES, Cne Ste CLAIRE-DEVILLE (EMA), Cne BRETAUD (CAB).	DICT 1895 type B (Guerre).
1896	Gal NIOX (Insp. T.M.)	— d° ? —	d° - moins Cdt PICQUART et Cne BRETAUD — plus Cne FRITSCH (EMA), Cdt ROBERT (CAB).	Organisation exercices.

Année	Président	Secrétaire	Membres	Décisions ou avènements
1899	— d° —	— d° ? —	d° - moins Cne Ste CLAIRE-DEVILLE — plus Cne SOURIAU (EMA).	Propose création bureau de décryptement (accordé mais menacé) DICT 1899 types 1 et 2.
1900	Gal PENEL (Insp. T.M.)	Cne CARTIER (21° BG)	?	?
1902	Cl BERTHAUT (EMA)	— d° —	Cdt JOSSE (chef EM XVIII° CA) - Lt-Cl de CHILLY (EMA).	Repousse système JOSSE (subst. double clé) organise cours (3 élèves).
1906	Gal BERTHAUT (sous-chef EMA)	Cdt CARTIER (EMA 2)	Cdt THEVENIN (EMA) - Cdt OLIVARI (19° Brigade d'Artillerie) CAZALAS (Armée des Alpes) - BASSIERES - LATREILLE - PAULIER.	Fusion chiffrement et déchiffrement.
1907	Gal BERTHAUT (sous-chef EMA)	Cdt CARTIER (EMA 2)	Cdt THEVENIN (EMA) - Cdt OLIVARI (19° Brigade d'Artillerie) CAZALAS (Armée des Alpes) - BASSIERES - LATREILLE - PAULIER.	Cdt GIVIERGE collabore avec Intérieur.

Année	Président	Secrétaire	Membres	Décisions ou événements
1909	— d° —	— d° —	— d° —	Création commission interministérielle.
1912	Gal de CASTELNAU (sous-chef EMA)	Cdt CARTIER (EMA - SR)	Cdt CAZALAS (EMA-2) Cdt OLIVARI (19° B. Art.) Cne LATREILLE (Sce Hist.) Cne PAULIER (76° RI) Cne BASSIERES (46° RI) Cdt GIVIERGE (GMP puis CAB).	Procédé SD 12. Création section du chiffre au Cabinet ; Nouveaux dictionnaires Paix et Guerre.
1913-1914	Gal BERTHELOT (sous-chef EMA)	— d° —	— d° —	