ASSOCIATION des RESERVISTES du CHIFFRE

Nouvelle Série – N° 4 – 1976

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

5ème Partie

LA GUERRE 1939 - 1945

Cette cinquième partie englobe deux phases actives 39-40 et fin 42-45 séparées par une phase d'attente; nous les examinerons successivement. Cette période n'apportera guère à l'Armée française de nouveautés sur le plan technique, sauf tout à fait à sa fin mais elle verra un accroissement des effectifs des chiffreurs, en relation avec le développement des Transmissions et par là, l'admission définitive et systématique des sous-officiers comme chiffreurs : les officiers, d'exécutants, deviennent des " directeurs ". Elle apportera par contre en 1943, un changement de structure opportun et de grande importance pour l'avenir.

5 - 1 39 - 40

5.1.1 - Organisation - Fonctionnement

La mobilisation voit la mise en place du dispositif et des moyens prévus; seules quelques petites difficultés de personnel se présentent, facilement résolues au cours de la longue phase d'attente. Celle-ci est mise à profit pour compléter l'instruction du personnel, mais elle ne laisse pas présager l'embouteillage qui sera celui de nombreuses sections dès le début des opérations, en mai 1940. Dès le premier jour de l'attaque allemande, en effet l'afflux des messages entraîne saturation, fatigue, erreurs et réclamations du Commandement, auprès duquel la " cote " du chiffre descend brutalement. L'insuffisance quantitative des moyens et du personnel est patente, sauf au G.Q.G. qui réussit à faire face.

Les mouvements très rapides de grandes unités vers l'ouest, après la rupture du centre du front ont un certain nombre de corollaires :

- le chiffre n'est pas au P.C. avancé ou tactique,

- les sections divisionnaires reçoivent avec retard les clés à utiliser avec les échelons supérieurs,

- les messages déchiffrés sont souvent caducs ou précédés de communications téléphoniques.

On peut donc dire brutalement que placé dans une situation difficile, le Chiffre a été peu utilisé et n'a pas servi efficacement au-dessous de l'échelon de l'Armée.

Dans le même temps, les écoutes des communications allemandes faisaient ressortir, jusqu'à l'échelon C.A., un emploi intensif du clair. De là à déclarer que le Chiffre était inutile, il n'y avait qu'un pas et beaucoup le franchirent, sans mesure, ne distinguant pas les primautés respectives de la vitesse et du Secret en fonction de la situation, et cette généralisation hâtive devait peser lourd dans les années suivantes.

5.1.2 - Décryptement

5.1.2.1 - La répartition des tâches demeura celle de la guerre 14-18, recherches, établissement des clés, décryptements et certains déchiffrements à l'E.M.A., quelques recherches et surtout déchiffrement au G.Q.G. (La Briarde); à cela s'ajouta le travail du S.R. installé au château de GRETZ où le Commandant BERTRAND avait réussi à adjoindre à un très petit noyau français l'équipe polonaise échappée au désastre et une équipe formée en grande partie de républicains espagnols.

5.1.2.2 - La section allemande de la section de l'E.M.A., sous les ordres du Commandant DUFILHOL traite plus de 40 000 messages pendant cette période, en liaison avec la section de l'Armée de l'Air. Outre le rétablissement de nombreuses clés de transposition, le résultat principal est le déchiffrement constant des messages utilisant le code en 3 lettres de la Luftwaffe, qui permettra de connaître, fin 39, l'implantation des escadres et de suivre sans interruption leur évolution.

5.1.2.3 - La section du G.Q.G. rencontra initialement de grosses difficultés car la "matière" à décryptement, c'est-à-dire les résultats des écoutes étaient généralement inexploitables.

Le Commandant JOUBERT des OUCHES par ses rapports personnels avec le Commandant BERTRAND et un représentant britannique, le Colonel TILTMAN, qui détacha trois décrypteurs anglais à la Briarde, réussit à donner de l'efficacité à sa section, et à l'Armistice, environ 9 000 messages en transposition double de la Luftwaffe, des Panzertruppen et d'Etats-Majors divers avaient pu être traduits et remis au 2ème Bureau.

5.1.2.4 - De son côté, le Général BERTRAND donne les renseignements suivants :

Le groupe de GOMETZ fut renforcé par la section du Chiffre de l'E.M.A. en avril 1940. L'unité du décryptement était enfin réalisée et l'effectif total se montait à 70. Il avait aussi des officiers de liaison britanniques et recevait les résultats des écoutes de l'Air et de la Terre.

Un effort fut appliqué au trafic des agents de renseignement allemands et, de février à mai 1940, 500 messages, soit un tiers du trafic intercepté, furent lus.

Mais l'effort principal resta sur l'Enigma, dont 40 exemplaires de copies furent commandés en France au début de 1940, elles étaient près d'être achevées à l'Armistice.

Les décryptements ne furent pas faciles ni permanents. Dans son ouvrage, le Général BERTRAND rapporte que d'octobre 39 à juin 1940, 141 clés furent reconstituées, permettant de rétablir

- 947 messages pendant 25 jours entre le 28.10.39 et le 9.4.40.

- 768 messages pendant 27 jours entre le 11.4.40 et le 12.5.40.

- 3074 messages pendant 22 jours entre le 20.5.40 et le 14.6.40.

Ces résultats ont été contestés ; certains pensent que le rétablissement des clés de l'Enigma fut assez exceptionnel, mais la réussite britannique, exposée en annexe, laisse à penser que les résultats pouvaient être obtenus manuellement et le furent.

Il est donc certain que l'équipe polonaise réussit, au moins dans des cas favorables, à décrypter un assez grand nombre de messages chiffrés avec l'Enigma et à rétablir les clés. Peut-être même, les Anglais communiquèrent-ils les clés trouvées par leur machine ?

5.1.3 - Un seul renseignement est actuellement connu sur les succès des décrypteurs allemands pendant cette période (1). On affirme que les Allemands interceptaient et décryptaient le trafic radio du Ministère de la Guerre avec ses subordonnés ; les clés changeaient toutes les 4 semaines et étaient retrouvées en peu de jours ; cependant, la clé mise en service le 10 mai 1940, n'aurait pu être rétablie. Cette dernière indication tend à faire croire que les succès allemands ne furent que partiels mais l'auteur certifie que les interceptions permirent de suivre l'ordre de bataille, encore qu'il appelle "détachement d'Armée", le groupe d'Armées A qui intervint en Belgique.

5.1.4 - La majorité des archives des sections furent détruites lors du départ de Paris et à l'Armistice, mais l'essentiel fut préservé à l'E.M.A. comme au S.R.

5 - 2 1940 - 1942

5.2.1 - Une des clauses de l'Armistice était le dépôt auprès des autorités allemandes de tous les procédés de chiffrement et clés utilisés, ainsi que la remise des nouvelles clés avant changement, aussi bien pour l'Armée de l'Armistice métropolitaine que pour les Forces d'Outre-Mer (y compris l'A.F.N.).

La section du Chiffre ne remit aux Allemands qu'une faible partie des informations réclamées et en particulier réussit à conserver secrets un assez grand nombre de dictionnaires et de codes.

Il n'était évidemment pas question d'utiliser des systèmes non déposés sur les Transmissions interceptables.

(1) source : der Geheimdienst in Europa 1937 - 1945, par Wilhelm von Schramm.

Des procédés secrets (vis-à-vis des Allemands et Italiens), furent mis en place (tels le nouveau code F.P. en 4 chiffres, désordonné, à utiliser avec un surchiffrement par transposition en septembre 1942, ainsi que des cles pour B 211 et C.36) avec les consignes d'emploi voulues. On peut noter aussi l'apparition du procédé manuel SD 38, de l'Armée de l'Air dérivé du SD 12, et mis en place dans l'Armée de l'Armistice en 1941.

On sait aussi que les services d'écoute et de radiogoniométrie du Colonel ROMON continuèrent à fournir au 2ème bureau des informations sur les forces allemandes, que le S.R. en transmit aux alliés, mais on ignore la participation éventuelle des personnels de la section allemande de la section du Chiffre, qui fut dissoute et son personnel dispersé à l'Armistice.

Une nouvelle fraction des archives, conservées en 1940, fut détruite lors de l'occupation de la zone sud par les Allemands et la dissolution de l'Armée de l'Armistice.

5.2.2 - Le S.R. continuait son travail, mais dans la clandestinité, le Commandant BERTRAND ayant réussi à installer ses équipes polonaise et espagnole dans une propriété du Sud du Massif Central.

Alimenté par les écoutes du Colonel ROMON et par ses écoutes propres, le S.R. réussit jusqu'en 1942 à décrypter 673 messages Enigma* et 4 500 messages en autres procédés. Après l'invasion de la zone sud en 1942, les services spécialisés de la Gestapo interceptèrent les messages radio émis vers Londres et les autorités polonaises en exil et manquèrent de peu l'arrestation de tout le groupe, qui put se disperser in extremis.

L'équipe polonaise parvint à gagner Londres via l'Espagne et apporta une aide importante aux Britanniques, avant de revenir en grande partie au sein de la D.G.E.R. en 1945 - 1946

* *Ce nombre relativement faible par rapport à celui de 1940 tient sans doute au faible trafic chiffré allemand à l'Ouest durant cette période et à la difficulté de rétablir manuellement les clés.*

5 - 3 1942 - 1945

5.3.1 - En Métropole, une section "fantôme" subsiste; les personnels restent en place ou en liaison, participant de près ou de loin à la Résistance, prêts à reprendre le service quand il en sera besoin. C'est ainsi que le Capitaine ARNAUD, sous les ordres du Commandant SERIES réussit, alors que les troupes allemandes envahissaient la zone sud, à dissimuler dans un château de l'Allier, 45 caisses de machines, dictionnaires et codes. En aout 1943, ce dépot parut en péril (les Allemands perquisitionnèrent en effet quelques jours plus tard et un fermier fut tué). Le Capitaine ARNAUD réussit avec l'aide de Monsieur PERRAUD, chargé officiellement de la récupération de produits industriels, à enlever ces caisses et à les dissimuler, après avoir brûlé en route près de 2 tonnes d'archives, dans une propriété de ce dernier. Récupérés en septembre 1944, les machines et dictionnaires ainsi préservés furent d'une grande utilité pour la remise en route du Chiffre métropolitain.

Enfin les officiers de la section du Chiffre composèrent, au profit soit du S.R. clandestin, soit de certains réseaux de la Résistance des procédés de chiffrement.

5.3.2 - Mais c'est en Afrique du Nord que le Chiffre renaît en même temps que l'Armée française, sous la direction du Général JOUBERT des OUCHES; celui-ci s'y trouvait depuis décembre 1940, comme Commandant en second puis Commandant du 7ème Régiment de Tirailleurs Marocains.

Il est appelé en décembre 1942 au cabinet du Général GIRAUD et prend le Chiffre en mains, aidé par le Colonel RAFFALI et le Lieutenant-Colonel LEGER.

Il s'agit de réunir ou de créer les moyens nécessaires, en personnels et en systèmes et d'en assurer la mise en place et le fonctionnement.

5.3.3 - Organisation et Personnel

L'organisme créé par le Général JOUBERT des OUCHES prend le titre de Direction Technique des Chiffres. Ses responsabilités ne concernent pas seulement l'Armée de Terre, mais tous les organismes gouvernementaux, aussi bien sous le Général

GIRAUD que sous le gouvernement provisoire du Général DE GAULLE , à l'exception des services spéciaux (BCRA puis DGER) qui conservent leur autonomie, et prennent aussi en charge toute la partie offensive, écoutes et décryptements, à l'exception des tâches opérationnelles (qui n'apparaîtront qu'en 1945).

Il s'agit d'une part de mettre sur pied un élément de direction et un atelier de chiffrement à ALGER puis d'équiper le 19ème corps, pour la campagne de TUNISIE, déjà amorcée.

Initialement (15.11.42 au 31.3.43), la section du chiffre du 19ème C.A. comprend 1 officier et 4 sous-officiers. Un cinquième sous-officier est affecté le 1.4.43 et la répartition des personnels est la suivante : P.C.avancé 1 of., 3 so.(dont 2 détachés auprés des alliés avec une C 36,) P.C. avant 1 so, P.C. arrière 1 so .

Dans les divisions, il y a un ou deux sous-officiers, sous la direction d'un officier du 2ème bureau, non spécialisé.

Les T.E.D. de 1943, qui restent en vigueur jusqu'à la fin de la guerre prévoient :

Armée : 3 officiers, 9 sous-officiers
Corps d'Armée : 2 officiers, 8 sous-officiers
Division : 1 officier, 5 sous-officiers.

Un problème extrêmement ardu fut de recruter et d'instruire les officiers et sous-officiers nécessaires à l'échelon central et dans les grandes unités, étant donné la pénurie générale en cadres. Ce ne fut pas une des tâches les moins difficiles du Général JOUBERT des OUCHES.

Ces officiers (parmi lesquels on peut noter le futur Général MULLER) et sous-officiers, sont formés partie sur le tas, partie au moyen de stages à ALGER, les "anciens" étant récupérés par priorité !

Le 2 février 1945 est créée par note EM GG/2 une section de déchiffrement à la 1ère Armée, qui comprendra une dizaine de personnes et sera alimentée par la Cie d'écoutes de la 1ère

Armée, par l'intermédiaire du 2ème Bureau.

A l'échelon central, il y a fusion de la Direction technique des chiffres et de la Section "guerre", jusqu'à septembre 1944, où la séparation sera concrétisée par la re-création de la Section.

La Direction technique se maintient sous une autre forme à partir de 1946 comme nous le verrons dans les parties suivantes.

Le T.E.D. de la Section du Chiffre de l'E.M.A. est le suivant, en octobre 1945 :

officiers : 12
sous-officiers : 14
A.F.A.T. : 24
P.C. : 18

Cette importance s'explique par l'intensité du travail de l'atelier de chiffrement et déchiffrement du Ministère ; dans les 5 derniers mois de la guerre, il a à traiter 18.000 messages soit une moyenne de 120 par jour, avec des pointes supérieures à 200, nécessitant la présence de plus de 20 chiffreurs, en raison des délais à respecter et des nombreuses fautes de chiffrement ou de transmissions à rechercher.

5.3.4 - Moyens techniques

5.3.4.1 - Le Général JOUBERT des OUCHES se trouve devant des codes compromis, des machines bien connues de l'adversaire ainsi que les procédés employés précédemment. En outre ces machines sont en nombre insuffisant ou très dispersées. Il s'agit donc, dans un premier temps :

- de faire l'inventaire des moyens existants
- de créer des procédés de surchiffrement ou de conditionnement (préambules des messages, indiquant les clés) suffisamment différents des anciens pour ne pas risquer de voir les Allemands déchiffrer facilement.

Dans un second temps:

- de redistribuer les moyens (machines en particulier)
- de faire imprimer de nouveaux dictionnaires et codes.

L'adoption de procédés de surchiffrement sérieux était gênée par l'abscence du personnel spécialisé.

Les nouveaux moyens seront les suivants :

- procédé SD 43, renouvelé du SD 12 et du SD 38
- code 72 (1943) - ordonné à 4 chiffres
- dictionnaire EMPIR (1943) désordonné à 5 chiffres
- code SAMOC (25.6.43) ordonné 4 chiffres
- genre SAMOC pour AOF en 1943
- code G.M.A. (AFN fin 42) à 3 lettres ou chiffres, utilisé seulement pour le camouflage
- "petit code" TRAMI (1943) à 5 chiffres utilisé, semble-t-il un peu comme le GMA, sans surchiffrement, la pagination variable étant fixée par 3 chiffres.
- code 75 (aout 1944) désordonné à 4 chiffres.
- dictionnaire EXTER (1944) semi-ordonné à 5 chiffres.
- dictionnaire LILIP (PUT) réalisé par photographies en très petit format, destiné aux officiers en mission.

Les conditionnements des messages en B 211 et C 36 sont refaits ; tandis que des nouveaux procédés de surchiffrement, sont utilisés avec les codes :

- clé additive courte, propre à chaque expéditeur pour le SAMOC
- transposition avec ou sans diagonales pour le code 72, toujours avec diagonales pour les dictionnaires EMPIR et EXTER
- substitution multiple pour le code 75.
- clés additives longues (carnets de clés).

La Direction technique des chiffres met également en place en 1943 un code pour les besoins de l'Intérieur, le code M.O.P. ; à 4 chiffres et pagination variable, mais le procédé de surchiffrement, s'il y en avait un, n'est plus connu.

5.3.4.2 - D'autres moyens sont en même temps utilisés par les forces françaises libres , le BCRA devenu DGER et les maquis.

On peut citer, pour les F.F.L.

- un code A.F.L. N° 1 à 5 chiffres, à pagination (3 chiffres) et chiffres des dizaines variables.
- un code utilisé au Moyen-Orient, comprenant 1.700

symboles de base, se présentant sous la forme d'une table à 80 colonnes de 17 lignes, l'élément chiffré à 3 lettres comprenant 1 consonne 1 voyelle et 1 consonne, la clé changeant tous les 20 ou 30 jours.

- pour mémoire le code A.T.M. utilisé par la colonne LECLERC.

Londres met en place, pour les besoins de l'Intérieur :

en 1941 un code F.L. à 4 chiffres, ordonné

en 1944 (?) un code F.F.I. N° 1 à 4 chiffres, ordonné,

tandis que la D.G.E.R. utilise en 1945 le code V à 5 chiffres. Seul semble-t-il, ce dernier système emploie un surchiffrement, par clé additive longue extraite d'un cahier.

Les agents de renseignements utilisent surtout des procédés mis en place par les Anglais, tels qu'un procédé de double transposition, les clés étant établies au moyen d'un poême et d'un nombre personnel.

Les maquis utilisent un code F.M.R., destiné aussi aux parachutistes, surchiffré par transposition.

Localement ils utilisèrent des systèmes trés variés et peu sûrs, tels que des mots conventionnels changeant peu souvent.

En outre les systèmes à clés blocs sont largement utilisés.

5.3.4.3 - Le Général JOUBERT des OUCHES arrive rapidement à équiper le 19ème C.A. en C.36 et parviendra même à doter certains échelons du niveau bataillon, mais l'équipement de nos unités ne sera vraiment complet que lorsque les Américains auront distribué leur machine M 209.

Cette machine M 209 d'invention HAGELIN également, se présente comme la C 36, mais comporte des améliorations sensibles : clé de rang plus longue, grâce à une sixième roue-clé et remontage de clé interne rendu plus difficile par la présence de cavaliers mobiles sur les réglettes.

Le corps expéditionnaire français en Italie et la 1ère Armée française seront alors équipés comme suit :

Liaison arrière (nationale) B 211 - code EMPIR

Liaisons internes (jusqu'au C.A.) B 211 - code 72

Liaisons internes (jusqu'au bataillon) M 209 - code 72
Procédé de secours et liaisons : SD 43

Une innovation très importante pour la sécurité du chiffre sera apportée en 1943 : le fractionnement des messages, qui fixe une limite maximale à la longueur d'un message chiffré avec une clé extérieure donnée et diminue ainsi les risques de recouvrement.

Parallèlement, le démarquage technique est généralisé et mieux appliqué, ce qui est très important au point de vue sécurité.

5.3.4.4 - A la libération les préfets nouvellement désignés reçoivent le code MOP, tandis que les régions militaires reconstituées sont dotées du code EMPIR ou EXTER avec un procédé de transposition à diagonales.

A la fin de la guerre enfin apparaissent à la 1ère Armée pour ses liaisons avec le Groupe d'Armées et dans les régions pour leur liaison avec l'administration centrale des machines américaines ou anglaises imprimantes à rotors.

5.3.4.5 - Il reste à parler du camouflage, problème toujours difficile. Résolu (et mal) par le code GMA en Tunisie, il reçoit deux solutions.

Dans les unités équipées par les Britanniques, comme la 2ème D.B., on emploie le SLIDEX, parfois jusqu'à l'échelon division ainsi qu'un système de mots conventionnels (cf le fameux message "TISSU est dans IODE" pour rendre compte de l'entrée des éléments avancés à Strasbourg), qui a l'inconvénient d'être rarement changé du fait de la difficulté de diffusion.

Dans les unitées rattachées aux Armées américaines, on utilise aussi des mots conventionnels et l'AFCODE. Cet AFCODE est le procédé officiel, c'est un code en bigrammes littéraux, désordonné, se présentant sous la forme d'une feuille imprimée au recto (ENCODE) et au verso (DECODE), difficile à lire, en raison de la petitesse des caractères, laissant un certain nombre de groupes disponibles pour la désignation des lieux et unités.

Il sera généralement peu employé, en raison de réticences peu justifiées, mais surtout de la difficulté de sa diffusion quoti-

dienne jusqu'aux plus petits échelons.

5.3.5 - Décryptement

5.3.5.1 - En dehors des travaux faits par la D.G.E.R. que nous ignorons, le problème de l'étude des messages interceptés par la compagnie d'écoutes et de radiogoniométrie de la 1ère Armée se pose (il ne s'était pas posé au 19ème C.A. ni au CEF, qui n'avait pas de moyens d'écoute spécialisé).

La décision 829 EMGG/2 du 2.2.45 crée une section de déchiffrement à la première Armée, placée sous les ordres du Commandant DUFILHOL.

Les chiffreurs allemands utilisaient à l'époque toujours l'ENIGMA et, comme procédés manuels, le HAND SCHLUSSEL et le RASTERSCHLUSSEL systèmes de transposition à trous réalisés au moyen de grilles utilisées en général une seule fois.

Aucun résultat ne fut obtenu à leur égard, mais par contre tous les messages interceptés camouflés soit au moyen du SCHLUSSELTAFEL (substitution simple sur code à 3 lettres) ou de répertoires à deux lettres furent décryptés ou déchiffrés. On note ainsi 119 messages traduits et remis au deuxième bureau entre le 25 mars et le 20 avril 1945.

A vrai dire, à la fin des opérations, peu de messages étaient réellement chiffrés ou camouflés et les procédés les plus divers étaient employés, généralement une substitution simple.

5.3.5.2 - Nous ne savons que fort peu de choses des décryptements opérés par les Allemands sur les communications françaises.

Un rapport allemand du 1.2.44 indique qu'en 1943, les messages échangés à l'intérieur des unités FFL de Syrie et interceptés étaient tous traduits sans difficultés et sans retard, alors que la liaison Syrie-AFN a résisté au décryptement.

Les systèmes percés étaient des moyens simples de camouflage et le code dont il a été question au paragraphe 5.3.3.2.

Il est certain que des moyens simples ne pouvaient résister aux Allemands qui disposaient de moyens importants : à l'échelon Armée, il existait en effet une section d'écoutes et

goniométrie mettant en œuvre 12 à 15 postes d'écoutes et ils avaient mis sur pied dès avant la guerre des services de décryptement importants. Il semble fondé de croire que les systèmes de surchiffrement par transposition à diagonales résistèrent.

Le livre allemand déjà cité (§ 4.4.5) indique que les Allemands possédaient la machine C.B. 38 vendue par HAGELIN aux Etats-Unis (sans doute la M 209 en terminologie américaine) et avaient assez vite reconnu sa mise en service. Son principe substitution à double clé à alphabets ordonnés avait permis la mise au point d'une méthode de décryptement. Il est donc vraisemblable que les messages chiffrés en M 209 purent être déchiffrés dans certains cas (trafic abondant). Un autre renseignement signalait aussi la présence d'une machine HAGELIN de ce type détenue par les Allemands au Portugal.

5.4 - TRANSMISSIONS ET CHIFFRE

Les relations Transmissions et Chiffre ne posèrent pas les mêmes problèmes qu'en 1914-1918 ; les questions d'interception et de décryptement étant réglées, il restait le problème de l'acheminement rapide et sans erreurs des messages à protéger.

En 1939-1940, le problème n'eut pas le temps de se poser, Transmissions et Chiffre se trouvèrent face à des problèmes analogues et y répondirent aussi mal.

Pendant ce qu'on pourrait appeler la pause (1940-1942) chacun tira ses propres enseignements de la campagne de mai-juin et chercha comment améliorer le service, mais il ne semble pas que des modifications de structure aient été avancées, quoique beaucoup d'officiers supérieurs des Transmissions pensassent que l'insertion des ateliers de chiffrement dans les centres de Transmissions permettrait de gagner beaucoup de temps.

La question fut posée très brutalement par un officier de liaison américain auprès des autorités d'Alger en 1943, le Colonel TULLY.

Il écrit le 6 décembre de cette année au Général MERLIN, Commandant supérieur des Transmissions, pour lui confirmer son étonnement d'avoir constaté la séparation entre Chiffre et Trans-

missions dans les Armées françaises et lui demander que la France s'aligne sur les Etats-Unis, où l'officier du Chiffre est un adjoint du Signal Officer et où les chiffreurs font partie du Signal Center, sous l'autorité du Chef de Centre. Il craint en effet des erreurs dans l'acheminement des documents et des retards dans l'exploitation des messages.

Le Général MERLIN soumet aussitôt la question à l'Etat-Major Général, avec un avis très favorable motivé, mais la décision de l'état-major fut négative (décision 772 EMP/LI du 25.12.43, signé GIRAUD).

Le problème fut également posé dans d'autres situations :

A la deuxième D.B., suivant les règles britanniques, le même véhicule abritait d'une part un officier d'état-major et d'autre part, dans le même compartiment le poste radio avec ses exploitants et un ou deux chiffreurs, réalisant ainsi une fusion Transmissions-Chiffre bien plus avancée que l'insertion de l'atelier de chiffrement dans le centre de Transmissions.

Enfin en maints endroits le Chiffre se montrait incapable d'avoir le même débit que les Transmissions aux heures de pointe, amenant ainsi des retards accrus par des attentes dans les bureaux du courrier et ressentis très fortement par le commandement.

5.5 - CONCLUSION

Le Chiffre reconnaît en 1940 n'avoir pas mieux servi que les autres armes ou services de l'Armée (ni plus mal). La misère et les contraintes de l'Armistice l'empêchent de progresser, mais il prend, lui aussi, les mesures nécessaires à la reprise des combats.

La résurrection de 1942 entraîne une activité intense qui se traduit par l'accroissement nécessaire des moyens, mais ceux-ci comme dans les Armées alliées d'ailleurs, ne répondent plus aux besoins des forces modernes en guerre de mouvement.

Nous emprunterons la conclusion de cette partie au rapport du Capitaine BRUEL, qui fut officier du Chiffre d'une division de la 1ère Armée :

"Le Chiffre est donc loin d'avoir pu suivre les Transmissions dans la voie des progrès techniques. Aussi s'est-il passablement essouflé au rythme des dernières batailles et sa réputation de lenteur, déjà solidement ancrée dans l'esprit de beaucoup en 1939, ne s'est pas amoindrie, au contraire".

DIRECTION DU CHIFFRE

1939 - 1945

Section du Chiffre de l'E.M.A.

6.3.38 au 29.8.40	: Cdt DIMIER de la BRUNETIERE
20.8.40 au 15.12.40	: Lt-Colonel JOUBERT des OUCHES
16.12.40 au 10.4.42	: Cdt PROUST
25.4.42 au 10.11.42	: Cdt SERIES
11.11.42	: Cdt DUFILHOL (1)

Direction technique des chiffres	**Section du chiffre de l'EMGG puis E.M.A.**
12.42 au 17.10.44 : Colonel JOUBERT des OUCHES	1.10.44 au 30.6.45 : Lt-Colonel RAFFALI
18.10.44 au 20.3.45 : Colonel SCHOTT	
21.3.45 au 6.1.46 : Colonel RAFFALI	10.7.45 au 1.12.50 : Lt-Colonel LEGER

(1) - Il semble que le Cdt DUFILHOL ait exercé une fonction de conservation de la section du chiffre en métropole du 11.11.42 au 30.9.44, date à laquelle il rentra dans la section jusqu'à son départ à la 1ère Armée, comme chef de la section dite de déchiffrement (début 1945).

LE DECRYPTEMENT DE L'ENIGMA PAR LES BRITANNIQUES (1)

La présente annexe déborde quelque peu le sujet de l'historique du Chiffre de l'Armée de Terre française, mais il a paru intéressant de l'inclure dans ce travail, car ses informations corroborent la réalité du décryptement de l'ENIGMA relaté par le Général BERTRAND. Elles montrent aussi l'importance de la communication au commandement des renseignements ainsi recueillis (confer le "télégramme de la Victoire" de 1918) et les précautions à prendre pour ne pas tarir une telle source.

DECRYPTEMENT DE L'ENIGMA.

En 1938, les Britanniques étaient moins avancés que les Français dans la connaissance de l'ENIGMA; du moins le Group Captain WINTERBOTHAM ne parle pas de contacts entre le S.R. français et le S.I.S. britannique jusqu'alors sur ce sujet.

En 1938, raconte-t-il, un jeune mécanicien polonais employé dans l'usine allemande qui fabriquait les ENIGMA est expulsé d'Allemagne et va rendre compte au S.R. polonais et au correspondant anglais du S.I.S. à VARSOVIE de tout ce qu'il avait observé. Ce jeune homme est envoyé à PARIS où il réalise un modèle en bois de la machine.

Le S.R. polonais monte avec l'agent anglais une opération qui permet de capturer une des machines en cours de production et de la faire parvenir à LONDRES (le Général Bertrand dit que le S.R. polonais avait construit lui-même des machines

(1) Ces renseignements sont extraits du livre "The ultra secret" de F.WINTERBOTHAM C.B.E., Group Captain de la R.A.F., ancien chef de la section AIR du "Secret Intelligence Service".

d'aprés les informations recueillies par les Polonais et les Français et envoyé à Paris deux machines dont une pour les Anglais).

Le service de décryptement anglais fait appel dès le début de la guerre à de grands mathématiciens, estimant que si L'ENIGMA crée un problème mathématique, une autre machine doit pouvoir le résoudre. Au début de 1940 ces mathématiciens réalisent à cet effet une machine électronique.

Fin Février 1940, la Lutwaffe avait reçu des ENIGMA et commencé un important trafic d'entraînement qui permit (sans doute grâce à des erreurs et des répétitions) de mettre au point la machine et sa méthode d'emploi et le premier décryptement fut réalisé en Avril 1940.L'ENIGMA navale, quelque peu différente de l'ENIGMA "Wehrmacht" fut décryptée peu après. Deux autres ENIGMA furent capturées en 1940, l'une en Norvège sur un avion allemand abattu, l'autre dans une unité allemande en Belgique, une troisième enfin sur un sous-marin allemand (avec instructions et clés) en Mai 1941.

Ceci permit de sophistiquer le calculateur et d'en fabriquer plusieurs mieux adaptés au début de 1942, en tenant compte des améliorations apportées par les Allemands à leur machine entre 1940 et 1942. On peut ainsi à partir de cette époque lire tous les messages interceptés en moins de deux heures, alors qu'il fallait parfois auparavant 24 heures. F.WINTERBOTHAM relate cependant un contact en Avril 1940 avec notre 2ème bureau (le général BERTRAND dit qu'ils furent fréquents sur le sujet en cause à partir de 1939) où se trouvait un détachement britannique et cite notamment le Colonel Philippe JOUBERT (notre Général JOUBERT des OUCHES). Il reconnaît enfin que les Français observèrent vis-à-vis des Allemands une discrétion totale en ce qui concerne l'ENIGMA mais ne parle pas du travail réalisé en FRANCE, ni de la venue de l'équipe polonaise à LONDRES en 1942.

EXPLOITATION DES RESULTATS

Dès le premier décryptement réussi, les Anglais se préoc-

cupèrent de la diffusion à donner aux informations ainsi acquises et de la protection de cette source qui devint incomparable comme d'ailleurs la lecture des messages russes par les Allemands dans la 2ème guerre mondiale, après la 1ère. Le nombre et la qualité des destinataires furent strictement limités, à l'échelon gouvernemental comme dans les Armées. W.CHURCHILL les recevait et appelait cela sa "most secret source". Les principes retenus furent d'utiliser des voies de transmission physiques ou électriques spéciales. Auprès des états-majors se trouvaient des détachements de liaison spéciaux (special liaison unit, S.L.U.), comportant des officiers et sous-officiers qui remettaient un exemplaire des messages à leur correspondant désigné et le reprenait ensuite pour l'incinérer.

Les officiers habilités des états-majors, comme les chefs, recevaient une instruction particulière sur la sécurité à respecter et la façon d'utiliser ces renseignements sans compromettre la source, c'est-à-dire sans donner à penser aux Allemands que leurs messages étaient lus.

Ces détachements de liaison étaient munis de postes radio leur permettant d'entrer dans le réseau du S.IS., à toute distance et les messages transmis étaient chiffrés d'abord au moyen de clés blocs (seul moyen réellement indécryptable initialement) puis avec la machine TYPEX.

Tous les documents relatifs à cette source et ceux qui en étaient issus portaient la mention spéciale "ultra secret" qui a donné son titre au livre précité.

RESULTATS OBTENUS

A partir de mai-juin 1940, tous les messages du haut commandement allemand passés par radio furent interceptés et déchiffrés. Comme HITLER avait centralisé le commandement de façon très étroite et que la très large majorité de ces messages étaient transmis par radio, les Anglais puis les Américains furent toujours parfaitement au courant et au jour le jour de l'ordre de bataille, des intentions des commandements allemands et des plans d'opérations ; une seule exception, l'offensive

von Rundstedt dans les Ardennes en 1945 pour la préparation de laquelle le silence radio fut absolu, ce qui causa une extrême surprise aux alliés, habitués à être informés des projets allemands assez tôt pour les contrecarrer sans peine.

Ces informations furent essentielles pour la bataille d'Angleterre, où elles permirent notamment de connaître les objectifs et modes d'action de la Lutwaffe, pour la bataille d'EGYPTE où elles facilitèrent la mise en échec des plans de ROMMEL, pour les campagnes de TUNISIE et de SICILE etc... Elles furent un facteur important du choix du lieu de débarquement en FRANCE et permirent, entre autres, de résister victorieusement à la contre-attaque de MORTAIN et de faire anéantir par l'aviation des divisions blindées en déplacement.

Ce livre signale un évènement curieux de la campagne de FRANCE en 1940. Le 23 mai fut intercepté et décodé un message de l'OKW prescrivant aux forces allemandes d'achever l'encerclement des forces alliées en BELGIQUE. W.CHURCHILL et Lord GORT eurent connaissance de ce message au moment où WEYGAND demandait que le corps expéditionnaire britannique participe à la contre-attaque NORD-SUD qui devait permettre de couper les forces allemandes en route vers la Manche de Boulogne. Craignant la destruction du corps expéditionnaire, CHURCHILL et GORT, au vu de ce message décidèrent alors de le replier sans retard sur Dunkerque, pour le réembarquer. Or cet ordre fut annulé sur place par HITLER qui voulait que ses unités soufflent et se réorganisent, de sorte que la non-participation des Anglais à la contre-attaque abandonnée en raison de leur défection serait due à ce "malentendu".

En ce qui concerne la guerre en Extrême-Orient, la machine décryptée par les Américains était dérivée des premières ENIGMA et les Japonais utilisèrent ensuite d'autres ENIGMA, de sorte que les Anglais n'eurent aucun mal à déchiffrer les messages japonais et les communiquer aux Américains. Un détachement de liaison important fut installé à BRISBANE, avec des moyens de déchiffrement, semble-t-il, et des détachements spéciaux firent parvenir les informations recueillies à Lord MOUNTBATTEN, à l'Amiral NIMITZ et au Général MAC ARTHUR

et à leurs subordonnés habilités, sans difficultés autres que celles des transmissions dans ce vaste théâtre d'opérations.

Pour clore ce récit, il suffit de citer le passage suivant d'une lettre adressée en juillet 1945 par le Général EISENHOWER au Général MENZIES, chef du S.I.S. britannique "L'information émanée de votre service avant et pendant cette campagne a été d'une valeur sans prix pour moi. Elle a simplifié énormément ma tâche de chef".