ECOLE DE PERFECTIONNEMENT

des Officiers de Réserve de Penthièvre

LE CHIFFRE

Conférence faite le 6 février 1927

par M. le Colonel d'artillerie breveté

GIVIERGE

Chef de la section du Chiffre à l'État-Major de l'Armée

ALLOCUTION

du Lieutenant-Colonel Directeur

Messieurs,

On a dit, quelquefois, en parlant de la victoire, qu'elle était fille du *secret* et de la *vitesse*.

Cette définition, dans cette forme expressive, souligne l'importance que l'on a toujours accordée au secret dans les opérations de guerre et également le souci que les différents échelons du commandement ont eu, à toutes les époques, de cacher à l'ennemi et leurs intentions et leurs dispositions.

Cette importance du secret dans les opérations militaires et ce souci de les masquer à l'adversaire n'ont cessé de s'accroître parallèlement aux progrès réalisés dans la puissance du feu et se sont particulièrement affirmés au cours de la dernière campagne.

Au temps de l'épopée napoléonienne où les fusils portaient à 200 et les canons à 800 mètres, le combat se déroulait sous les yeux du chef et la transmission des ordres et des renseignements, faite par des estafettes, était chose relativement facile et sûre.

A notre époque de progrès scientifiques intenses et où la puissance du feu est formidable, cette transmission des ordres et des renseignements est devenue singulièrement délicate et il a fallu substituer à l'estafette des moyens mécaniques, *téléphone, télégraphe, radiotélégraphie* dont la mise en œuvre, et c'est là la rançon même du progrès, exige des cadres des connaissances particulières et des précautions spéciales.

C'est un fait que lorsque, par exemple, on téléphone sur le champ de bataille ou lorsqu'on fait usage de la T. S. F., l'ennemi, par des appareils spéciaux, peut capter les communications et en déceler les intentions de l'adversaire. D'où la nécessité de faire usage de procédés rendant incompréhensible à l'ennemi le texte qu'il aura pu recueillir. Ces procédés constituent ce que l'on appelle le *chiffrement*.

Il importe que le *commandement*, à tous les échelons, se rende compte de l'obligation de chiffrer et, qu'en particulier,

le personnel des transmissions sache que le seul procédé réglementaire pour les correspondances par radio est le *télégramme chiffré*.

Dès le temps de paix, la troupe et les états-majors doivent être habitués à chiffrer et ce dressage doit s'effectuer dans tous les exercices sur la carte et sur le terrain, lorsque les effectifs fictifs ou réels correspondent par leur importance aux conditions normales d'emploi du chiffrement en temps de guerre, c'est-à-dire toutes les fois que la T. S. F. et la T. P. S. sont en jeu.

Sans doute, Messieurs, un certain nombre d'officiers sont spécialisés dans ces questions du chiffre. C'est le cas, en particulier, de vos camarades de l'Ecole de perfectionnement du Chiffre, qui ont bien voulu être des nôtres ce matin, et que je suis heureux de saluer, en votre nom. Ces officiers auront à dresser, à la mobilisation, le personnel sous-officiers et secrétaires qui constitueront leurs ateliers.

Mais, en outre de ces officiers spécialisés, dans les corps de troupe, les officiers chargés des liaisons et transmissions, les officiers de renseignements, tous emplois qui incomberont à beaucoup d'entre vous, à la mobilisation, doivent être également exercés à la pratique du chiffrement. C'est dans ce but que les corps de troupe ont été dotés de la notice du 1er juillet 1924 sur *les procédés de chiffrement dans les petites unités*.

Ces considérations vous expliquent, Messieurs, les raisons pour lesquelles nous avons prévu, dans notre plan d'instruction, une conférence sur le chiffre.

Pour traiter un sujet aussi délicat, tout à fait nouveau pour la grande majorité d'entre vous et vous en exposer les points essentiels, aucun officier n'était plus autorisé que *M. le colonel Givierge*, chef de la Section du chiffre à l'Etat-major de l'armée.

M. le colonel Givierge, malgré les lourdes obligations qui lui incombent, a bien voulu répondre à notre appel et venir en personne, avec la haute autorité qui s'attache à ses fonctions et sa longue expérience en la matière, vous exposer ce qu'il convient que vous sachiez des procédés de chiffrement actuellement en vigueur.

Je suis votre interprète, Messieurs, en lui exprimant toute votre reconnaissance, et, en y joignant mes remerciements personnels les plus respectueux et les plus vifs, je le prie de vouloir bien prendre la parole.

LE CHIFFRE

I. DEFINITION ET RAISON D'ETRE DU CHIFFREMENT

Messieurs,

Les conditions de la guerre actuelle et les engins agressifs nouveaux ont fait sur le champ de bataille moderne une large part au machinisme. Le domaine de la liaison n'a pas échappé à cette nécessité. Tandis que du temps de Napoléon le commandant en chef suivait dans sa lunette les mouvements des troupes, et faisait porter ses ordres par ses aides de camp, l'étendue du front, la profondeur de la zone dangereuse, l'obscurité pour les attaques de nuit, la fumée, la poussière et les gaz opaques pour celles de jour, la progression de trou d'obus en trou d'obus imposée par la puissance du feu, l'obligation pour l'assaillant de se dissimuler aux vues des aviateurs, nécessitent la transmission du renseignement depuis les observateurs placés dans les lignes jusqu'au commandement devenu presque aveugle, et la difficulté et la lenteur de la marche dans la zone de combat a fait préférer l'emploi du moyen mécanique qui porte l'ordre près de l'exécutant à celui des estafettes et des coureurs, tout au moins pour les longs trajets.

L'usage des matériels de transmission du genre téléphone, télégraphe ou radiotélégraphe a donc pris dans la dernière guerre un grand développement. Tous ceux d'entre vous qui ont lu l'historique de certaines luttes acharnées, comme les combats autour de Verdun, ont pu voir que, tout comme les autres matériels exposés au feu, ces instruments délicats ou bien exigeant pour leur mise en œuvre de longs fils ou des antennes d'une longueur et d'une élévation qui les rendent vulnérables, avaient manqué quelquefois à leur tâche, et que le coureur était alors resté le seul organe de transmission, souvent arrêté par la mort. Après la guerre on a cherché à rendre le matériel moins fragile et moins encombrant, on a étudié pour lui les

perfectionnements que la science des ondes a rendus nombreux depuis quelques années, on en a enfin augmenté les dotations. Certains esprits chagrins font bien des réserves sur les résultats qu'on en pourrait attendre, surtout au début d'une guerre. Ils font observer que pour la T. S. F. par exemple, nos appareils en usage exigent un personnel de lecteurs du Morse au son, pour ne parler que de celui-là, que notre service à court terme ne paraît pas fournir dans l'état actuel des choses, et que la multiplication des radio-concerts n'augmentera sans doute guère, bien que j'aie entendu verser cet argument au débat. Mais, à suivre les exercices sur la carte, les manœuvres sur le terrain où souvent d'ailleurs, la question des transmissions, bien que déclarée importante dans le thème, est traitée d'une façon extraordinairement sommaire dans la pratique parce qu'elle retarde le développement d'une manœuvre tactique ou stratégique dont on a hâte d'admirer le couronnement, on constate que notre commandement, à tous les degrés, semble considérer l'emploi du téléphone, de la T. S. F. et de la T. P. S. en guerre comme courant et d'exécution facile et rapide. Je ne parle pas de la télégraphie par fil, réservée pratiquement aux grandes unités et à un personnel particulièrement spécialisé.

Nous admettrons donc ici, pour traiter de la question du chiffre, que le personnel des transmissions, qu'il appartienne, dans les Etats-majors des grandes formations, aux unités de sapeurs-télégraphistes, ou, dans les corps de troupe, à l'effectif du corps lui-même, où il a été dressé par des instructeurs formés dans un centre de transmission régional ou à l'Ecole des liaisons et transmissions de Versailles, est parfaitement au courant de son service, et qu'il est capable, non seulement de recevoir des textes en langage courant, où l'erreur sur quelques lettres ne cause ordinairement que des fautes d'orthographe sans rendre le message incompréhensible, mais aussi des groupes de lettres ou de chiffres, où les erreurs risquent d'avoir des conséquences beaucoup plus graves.

Une des caractéristiques, bien fâcheuse, du matériel mis à la disposition de notre personnel, c'est que ce matériel est indiscret, et qu'au lieu de garder pour le seul destinataire le message qu'on lui confie, il le laisse entendre à tous ceux qui s'y intéressent. Le téléphone demande, pour ne pas faire fonctionner les écouteurs des appareils de captation ennemis, des conditions d'isolement, de double fil, etc., qui furent bien rarement, dans la pratique, respectées aux fronts de 1917 et 1918 ; l'optique envoie ses éclairs lumineux vers l'ennemi ; la T. S. F. et la T. P. S. rayonnent leurs ondes dans toutes les directions, et souvent, si l'on n'opère pas à énergie strictement suffisante, à des distances considérables. Je ne parle pas du télé-

graphe avec fil ; ses conditions d'emploi rendent les interceptions ou très faciles, parce que nous entrons dans les questions d'espionnage, ou assez difficiles pour que nous n'en tenions pas compte dans cette conférence destinée aux officiers des corps de troupe. Sans doute, on cherche des appareils n'ayant pas ces inconvénients, des matériels ou des dispositifs qui rendent l'écoute ennemie impossible. J'ai souvenance d'avoir fait jadis un travail d'étude sur les cuirasses des navires, et sur la lutte entre l'obus et ces cuirasses. Je crains de voir se renouveler, le cas échéant, une lutte analogue entre celui qui lance les ondes dans l'espace, et celui qui cherche ou à les recueillir ou à les arrêter.

Ainsi, lorsqu'on téléphone au voisinage du front, lorsqu'on émet un signal de T. S. F., il faut admettre que l'ennemi nous écoute, et, si nous ne voulons pas qu'il nous comprenne, il faut trouver un moyen pour que le texte que nous confions à l'appareil ne soit compréhensible que pour le destinataire, sans que les indiscrets aux mains desquels il pourra tomber puissent se renseigner à sa lecture. Le procédé par lequel un texte n'est compréhensible qu'aux gens pour lesquels il a été établi, alors qu'il reste un rébus aux yeux des autres, constitue le chiffrement. La convention établie entre l'expéditeur et le destinataire, au moyen de laquelle ce dernier extrait du rébus le renseignement ou l'ordre qui lui est adressé, constitue la clef. Les procédés les plus propres à donner des solutions convenables des problèmes de chiffrement, tant pour fournir à l'expéditeur et au destinataire des moyens simples et efficaces de protéger leur correspondance, que pour permettre aux spécialistes ennemis de retrouver les conventions et les clefs et d'arriver ainsi à lire des textes chiffrés dont on voulait leur cacher le sens, ressortissent d'une science particulière qu'on appelle la *cryptographie*.

II. QUELQUES MOTS DE CRYPTOGRAPHIE

Je ne traiterai pas, dans cette conférence, de la *cryptographie* au point de vue général. Je ne ferai qu'indiquer quelques principes pour préciser les procédés employés dans notre armée, et ne pas laisser croire qu'il n'en existe point d'autres.

Les procédés *cryptographiques* sont extrêmement nombreux : il en est qui, faisant appel soit à des caractères d'écriture de forme particulière, soit à des conventions spéciales sur des intervalles entre les lettres d'un texte ou à des fautes d'orthographe volontaires, exigent que le destinataire travaille sur le texte écrit de la main même de l'expéditeur. On ne s'intéresse dans l'armée qu'aux procédés qui peuvent emprunter la voie télégraphique, c'est-à-dire qui n'utilisent que les chiffres ou les lettres de l'alphabet usuel de la langue employée,

laquelle doit rentrer dans le nombre de celles qu'a admises la convention internationale pour les transmissions télégraphiques.

Qu'il s'agisse de ces procédés ou de ceux, mentionnés ci-dessus, qui ne peuvent être utilisés par le télégraphe, mais peuvent figurer dans des lettres (et nous ne parlons pas des encres sympathiques), on répartit généralement les procédés crytographiques en deux grandes classes : substitution, transposition.

Dans les procédés de *substitution,* les lettres du texte à chiffrer, du texte qu'on appelle texte clair, sont remplacées par d'autres lettres, ou par des groupes de chiffres, ou par des groupes de lettres, ainsi ENNEMI pourra être chiffré KXXKZT ou AM. BI. BI. AM. RZ. VT. ou 12, 31, 31, 12, 45, 03. On voit dans ces exemples que les deux lettres E du mot ENNEMI d'une part, les deux lettres N du même mot d'autre part, sont représentées par un même caractère K, ou AM, ou 12 pour E, X ou BI ou 31 pour N. Il est des procédés de substitution plus compliqués où, par l'emploi de plusieurs tableaux de correspondance, on n'observe plus cette particularité : une lettre du clair n'a pas qu'une représentation dans le *cryptogramme,* elle en a tantôt une, tantôt une autre, suivant sa place dans le texte. Dans les systèmes de substitution l'ordre des lettres n'est pas changé : le premier signe du crytogramme représente la première lettre du texte clair, le dernier correspond à la dernière lettre.

Dans les procédés de *transposition,* les lettres ne sont pas modifiées, mais on en change la succession, de telle sorte que pour traduire le *crytogramme* il faut avoir la clef qui permet de remettre en ordre une suite incohérente de caractère, JE VAIS A PARIS donnera par exemple SPAAIAVJESJR.

On peut d'ailleurs combiner ces deux procédés fondamentaux, et, après avoir changé par substitution les caractères du texte clair en d'autres caractères, mélanger ceux-ci par une transposition, ENNEMI AM. BI. BI. AM. RZ. VT., pourra alors devenir ABBAMIIMRTZV par exemple. Certains de ces procédés sont très sûrs, d'autres le sont moins ; certains sont simples, d'autres sont compliqués et exigent plus de temps pour le chiffrement et plus d'attention des chiffreurs.

Je ne vous parlerai pas des procédés employés pour essayer de trouver les clefs et les traductions des cryptogrammes de cette nature. Il y aurait dans tout cela : études détaillées des systèmes crytographiques, considérations historiques sur leur emploi, procédés de décryptement (opération de traduction de cryptogrammes dont on n'a pas la clef) études pour établir des machines à chiffrer analogues comme emploi à des machines à écrire, la matière d'une conférence assez longue, et, j'ose le dire, intéressante.

Les procédés de *substitution* et de *transposition* où l'on modifie, ou bien où l'on mélange les lettres des textes en les prenant une à une, quelquefois deux à deux, sont appelés souvent procédés littéraux ou numériques. Ils ont en général l'avantage suivant : un chiffreur connaissant le procédé par cœur, et se souvenant de la clef, n'a besoin que de papier et d'un crayon pour transformer le texte clair en texte chiffré sans porter sur lui aucun document, dont la perte puisse renseigner l'ennemi et lui permettre de déchiffrer. Ils ont l'inconvénient d'exiger en général des chiffreurs une certaine instruction technique assez développée. Aussi, alors qu'avant 1914 la plupart des puissances avaient adopté pour *leur correspondance cryptographique militaire de campagne* des procédés de ce genre, la plupart aussi y ont renoncé pendant la guerre pour adopter des systèmes qu'on a cru pouvoir mettre sans inconvénient entre les mains des premiers venus, c'est-à-dire pour mettre en service des dictionnaires chiffrés.

Les procédés à dictionnaire exigent la possession par l'expéditeur et le destinataire d'un même document, appelé suivant la fantaisie des auteurs et des imprimeurs, dictionnaire chiffré, code chiffré, répertoire, carnet de chiffre, table, etc... Ce document est un dictionnaire où les mots sont rangés, comme dans tout dictionnaire, en une liste par ordre alphabétique. Pour chiffrer, on emploie un système de substitution ; on remplace les mots par des groupes de chiffres ou de lettres, et, en face de chaque mot dans le dictionnaire se trouve le groupe de chiffres ou de lettres par lequel on le représentera dans le texte chiffré. Quand il doit chiffrer un texte, le chiffreur cherche dans la liste le mot du clair à sa place alphabétique, il lit en face un groupe de chiffres, et l'écrit pour former le cryptogramme. Pour déchiffrer, le destinataire cherche le groupe de chiffres du crytogramme, et écrit le mot clair qui figure en face. Dans certains dictionnaires, la liste des groupes est ordonnée numériquement comme la liste des mots est ordonnée alphabétiquement. On aura : A = 000, ABBE = 001, ACCEPTER = 002, etc., ZONE = 998, ZOUAVE = 999. Ce seul tableau de correspondance entre mots du clair et groupes servira au chiffreur et au déchiffreur, qui trouveront sans hésitation les mots et les groupes à leur rang. Mais au point de vue cryptographique, un tel document n'est pas sûr : si j'arrive par espionnage ou autrement, à savoir qu'un groupe 002 veut dire ACCEPTER je serai sûr que les groupes 001 et 000 correspondent à des mots alphabétiquement placés avant ACCEPTER. Je serai certain, d'autre part, que 997 ne voudra pas par exemple dire ADJUDANT, parce qu'il correspond à un mot dont la lettre initiale se trouve vers la fin de l'alphabet. On a cherché à éviter cette cause de faiblesse, et pour cela on a supprimé tout ordre dans la correspondance des mots et des grou-

pes. On aura par exemple A = 851, ABBE = 652, ACCEPTER = 085, ZOUAVE = 436. La connaissance du sens de 085 ne nous dit plus rien pour celui de 084, ni pour les groupes représentant A et ABBE. C'est bien plus sûr. Mais tandis que le chiffreur trouve toujours ses mots à leur place alphabétique, le déchiffreur n'a plus aucun fil d'Ariane pour trouver ses groupes, il est obligé de les chercher dans la longue liste où ils sont répartis au hasard. On fait alors une deuxième liste, où les groupes sont par ordre numérique, avec leur sens dans un ordre qui est quelconque et non plus alphabétique. On a par exemple 000 = CHIEN, 001 = NAVIRE, ... 998 = DELIT, 999 = VIDE. Le chiffreur opèrent sur un tableau, le déchiffreur sur l'autre, et le dictionnaire est dit « à deux tables » table chiffrante et table déchiffrante. C'est plus sûr, et avant 1914 on regardait ce procédé comme absolument sûr, mais il y a deux fois plus de pages et il faut vérifier avec beaucoup de soin le collationnement des deux parties lors de l'impression, sinon un groupe a un sens au chiffrement et un autre au déchiffrement.

Nos documents réglementaires sont tous, actuellement, du type dictionnaire à deux tables. Seulement, ils sont plus ou moins gros, contiennent d'autant plus de mots et d'expressions composées de plusieurs mots, sont plus ou moins « riches », qu'ils sont destinés à des autorités plus hautes dans l'ordre hiérarchique.

On ne met pas, en effet, dans ces dictionnaires, tous les mots d'une langue avec toutes leurs flexions grammaticales. On n'y place que les mots les plus utiles. Si l'on décide d'employer des groupes de 3 chiffres, on ne peut mettre que mille mots. On trouve alors dans le texte clair des mots qui ne figurent pas dans le dictionnaire : pour les chiffrer, on les coupe en syllabes ou même en lettres isolées suivant que le dictionnaire renferme les syllabes correspondantes ou seulement ces lettres. Il contient toujours, pour être utilisable, au moins ces dernières.

Alors, plus le dictionnaire sera riche, plus il y aura de chances que l'on n'ait pas besoin, au moins pour les mots du langage courant, de recourir à ce procédé qu'on appelle le « syllabage ». On sera, par contre, presque toujours obligé de l'adopter pour les noms de petites localités ou ceux de personnes, qu'on ne peut faire figurer dans les documents imprimés le plus souvent à l'avance, sans qu'on sache où se passeront les événements à l'occasion desquels ces documents seront utilisés, ni les noms des acteurs. Et c'est là, au point de vue de sécurité *cryptographique*, comme nous le verrons plus loin, une cause de faiblesse des dictionnaires, surtout des petits avec lesquels la décomposition doit souvent être poussée jusqu'aux lettres, les syllabes n'y figurant pas, faute de groupes disponibles pour les représenter. Par contre, les petits documents coûtent moins

d'argent et moins de temps à imprimer que les gros, et on est parfois obligé de les utiliser malgré l'inconvénient dont il s'agit, quand on est contraint de se limiter dans l'importance de documents qu'on aura à distribuer à des parties prenantes très nombreuses et exposées à les perdre, ce qui entraînera des remplacements fréquents.

Bien qu'on ait adopté les procédés à dictionnaire comme particulièrement simples, et utilisables, avons-nous dit plus haut, par le premier venu, l'expérience a prouvé par la suite que la négligence de certaines précautions facilitait pour l'ennemi la traduction des textes chiffrés avec un dictionnaire, et qu'il faut que le personnel connaisse ces précautions. Disons donc un mot des procédés que l'on utilise pour établir les traductions de cette nature.

Pour *traduire un télégramme chiffré avec un dictionnaire*, le plus simple est d'avoir un exemplaire du dictionnaire en sa possession. C'est une circonstance qui se présente quelquefois : on prend un dictionnaire au cours d'une retraite de l'ennemi ou à l'occasion d'un coup de main. En temps de paix même, les services d'espionnage s'efforcent d'obtenir des fragments des dictionnaires quand on les imprime, ou de se faire prêter un exemplaire par un secrétaire indélicat pendant le temps nécessaire à une photographie.

Quand on ne jouit pas de cette situation particulièrement favorable, on essaie de reconstituer le dictionnaire. La possession d'un document en clair et de sa traduction en chiffre est à ce point de vue fort intéressante, parce qu'en comparant ces deux textes on arrive à découvrir le sens d'un certain nombre de groupes. On a beau prescrire de ne jamais écrire la traduction d'un cryptogramme sur la feuille où figure celui-ci, donner l'ordre de brûler tous les brouillons qui ont servi à un chiffrement, de ne garder dans les archives que des papiers sans l'indication : « Traduction de télégramme chiffré » et sans indication d'heure et de numéro permettant de rapprocher ce texte clair du radiotélégramme de transmission écouté par l'ennemi, etc..., on a observé au cours de la dernière guerre des imprudences continuelles à ce sujet. Pour les télégrammes diplomatiques, les journaux donnent parfois des textes clairs, et dans la dernière guerre certains ambassadeurs se firent envoyer en chiffre le récit des événements militaires dont le communiqué en clair donnait des fragments, toutes imprudences qui, lorsqu'elles sont reconnus, facilitent la tâche des décrypteurs ; toutes imprudences que je vous signale pour que, vous conformant aux instructions réglementaires, vous les évitiez le cas échéant.

Lorsqu'on n'a pas d'éléments de cette nature, on s'attaque aux *cryptogrammes* par voie simplement technique. On note sur des cahiers l'apparition de chaque groupe de chiffres. On cons-

tate s'il est fréquent ou rare ; on fait le tableau des groupes qui le précèdent et qui le suivent, et souvent on s'aperçoit que certains groupes isolés reparaissent fréquemment (*ce sont des ponctuations, des prépositions, des articles, des verbes auxiliaires,* etc.), et que certaines séries de groupes se suivent dans le même ordre, reviennent plus ou moins souvent. Or, des séries de ce genre sont ordinairement dues à des mots qui ne se trouvent pas dans le dictionnaire, à des syllabages. Supposons que nous ayons un dossier de télégrammes émanant d'un point voisin d'une ville, *Florence* par exemple, où a lieu une conférence diplomatique à laquelle assistent MM. *Lorentz, Lerévérend, Rengerlo,* etc... Le chiffreur ne trouvant pas ces noms dans le dictionnaire aura pu chiffrer par syllabe.

F. LO. R. EN. CE.	217. 451. 728. 192. 105.
LO. R. EN. T. Z.	451. 728. 192. 845. 996.
L. ER. EV. ER. EN. D.	412. 198. 201. 198. 192. 132
R. EN. G. ER. LO	728. 192. 325. 198. 451

En retrouvant ces séries de chiffres, le spécialiste cherchera à quoi elles peuvent bien correspondre, et se reportera aux noms qui figurent probablement dans les télégrammes. Les deux ER de Lerevérend lui indiqueront l'hypothèse à faire sur les deux 198. Il en tirera une nouvelle sur 192 : EN, qui ouvrira une nouvelle porte par la présence de ce groupe dans les autres noms, la valeur de l'hypothèse se confirmant par les éléments de ceux-ci tels que 541 = LO, qui se trouvent à la place où on les attendait. De plus, la succession 192 : EN, 198 : ER, 201 : EV, lui donnera l'idée que le dictionnaire présente des groupes numériquement ordonnés. Si alors le groupe 000 est fréquent, il l'identifiera avec A. S'il trouve souvent les groupes 413, 418, 425, compris entre 412 : L, et 451 : 10, il en fera LA, LE, LES, et il devinera petit à petit, en se guidant sur la place du mot supposé dans l'alphabet, parallèle à la place du groupe dans la liste numérique, le sens des autres groupes du texte.

Si l'on avait employé un dictionnaire à deux tables, on aurait bien pu deviner le sens des séries de groupes, mais l'ordre numérique n'aurait servi de rien pour étendre le nombre des groupes traduits. On y arrive pourtant, bien qu'avec plus de difficultés, en s'appuyant sur la place des mots dans une phrase, sujet souvent pronom, verbe souvent auxiliaire, etc... et sur les renseignements recueillis dans les journaux ou dans les rapports d'agents.

Nous retiendrons de ceci que la présence dans un texte de séries de groupes se suivant dais un même ordre, de « *répétitions* », est un gros danger pour le secret. Il est donc recommandé aux chiffreurs d'éviter les *répétitions* : pour cela on peut couper les mots en *syllabes,* d'une manière différente d'une fois à l'autre. Si la suite 217, 451, 728, 192, 105 se répè-

tant trois fois, amène l'hypothèse FLORENCE, nous chiffrerons une fois F. LO. R. EN. CE, une fois FL. OR. NC. E., et une autre fois F. L. O. R. E. N. CE. ; comme cela il n'y aura de répétition que d'un ou deux groupes, qui n'attireront pas l'attention parce que cela se produirait souvent (indication pluriel, indicatif présent, etc... suivant un mot). Ce sera plus long à chiffrer, il faudra se donner la peine d'y penser, mais cela sera plus sûr.

On conçoit facilement que plus on aura de textes, plus on aura de chances de retrouver ces séries de mots ainsi que toutes les particularités qui peuvent guider le *décrypteur*. Dans un texte unique et court il y aurait peu de chances pour qu'il y ait des répétitions, car, si même les noms se répètent, on pensera à les syllaber différemment. Si les textes se multiplient, il n'en est plus de même. En particulier, la sécurité due au soin de syllaber de façons différentes, suffisante quand on a un seul chiffreur, s'évanouit pour un procédé de chiffrement du front en guerre, car si le chiffreur A fait attention de ne pas chiffrer deux fois F. LO. R. EN. CE., le chiffreur B. le chiffreur C. etc... ne savent pas quel chiffrement A a adopté. De plus, quand il y a beaucoup de textes, on finit par être obligé de reprendre un chiffrement déjà employé. Il a donc fallu trouver un autre moyen d'assurer la sécurité ; on a utilisé des surchiffrements.

Un surchiffrement est un procédé *cryptographique*, en général *substitution* ou *transposition*, qu'on applique sur la suite des groupes obtenus par le premier chiffrement dérivant directement du texte clair, qu'en cas d'emploi du dictionnaire nous appellerons chiffrement simple. Par exemple un procédé par substitution est le suivant. On établit un tableau où chaque chiffre de 0 à 9 correspond à deux ou trois lettres de l'alphabet, et on convient de remplacer les chiffres par une de ces lettres, tantôt l'une, tantôt l'autre. Chaque lettre au déchiffrement sera remplacée par le chiffre unique auquel elle correspond et on reformera ainsi les groupes tirés directement du dictionnaire. Alors, avec le tableau ci-dessous.

0	1	2	3	4	5	6	7	8	9
C	F	A	G	I	B	J	D	E	H
K	L	R	P	S	V	M	O	X	T
	U		Q		Y	N		Z	

notre série représentant FLORENCE 217, 451, 728, 192, 105 deviendra une fois AFD IBL DRE LHA UKV, une autre fois RUO SVU OAZ UTR FCB, ce qui ne révèle en rien la répétition du même mot.

Le *surchiffrement* est donc un procédé, augmentant, à vrai dire, la durée du travail du chiffreur, puisque c'est une opération supplémentaire, mais augmentant énormément la sécurité. D'autre part, un tableau de surchiffrement, comme celui que

nous venons d'établir, tient sur une feuille de papier et s'imprime en quelques heures. On peut donc changer un tel tableau, sans changer le dictionnaire, à peu de frais d'argent et de temps, et rendre une sorte de virginité à un document un peu suspect. En modifiant le surchiffrement d'un télégramme à l'autre, on réduirait à un seul texte le dossier du décrypteur, qui doit travailler sur un aussi grand nombre possible de documents de même clef, et par suite on donnerait à la correspondance une sécurité presque absolue. C'est ce qui se fait maintenant dans certains postes de chiffrement, au grand désespoir des bureaux de décryptement.

III. ORGANISATION ET EXECUTION DU SERVICE DU CHIFFRE AUX ARMEES

Ces notions sur les dictionnaires, et sur les motifs de certaines précautions rendues réglementaires pour leur emploi, étant exposées, passons maintenant à ce qui nous intéresse directement, à l'emploi des dictionnaires dans notre armée.

Comme nous l'avons dit, bien qu'on ait cru d'abord qu'on pouvait mettre ces documents dans les mains de n'importe qui, l'expérience a prouvé que « n'importe qui » s'en sert ordinairement mal. Pour que les chiffrements soient vite exécutés, que les précautions soient prises, que le déchiffrement ne se trouve pas arrêté par une petite erreur de transmission, il est nécessaire de spécialiser le personnel chargé du chiffre. A la suite d'une réunion des représentants des Etats-majors d'armée au G. Q. G. en 1918, on rendit réglementaire pour toute l'armée française une mesure déjà prise dans plusieurs grandes unités, et on créa des ateliers de chiffrement dans chaque corps de troupe et état-major disposant d'un poste de communications radioélectriques. Les tableaux d'effectifs actuels ont sanctionné cette création. Le chiffrement doit donc, en théorie, être assuré par des spécialistes. Mais actuellement, dans la pratique, les spécialistes manquent.

On a bien préparé des chefs d'ateliers de chiffrement pour les Etats-majors. Des officiers de réserve ont suivi les cours de l'Ecole d'Instruction du chiffre à l'Etat-major de l'armée, et ont été ainsi mis au courant de leur technique professionnelle. Ils auront pour mission de dresser le personnel, quelques sous-officiers et secrétaires, qui formeront leur atelier à la mobilisation, et qui n'ont jusqu'à présent reçu aucune notion de leur métier, d'exécuter le travail de chiffrement de leur Etat-major, et de guider et de contrôler le chiffrement dans les unités placées sous les ordres du commandement auquel ils appartiennent. Si un personnel analogue avait été préparé dans les corps de troupe, si toutes les prévisions relatives à l'organisation des

ateliers de chiffrement étaient réalisées, on pourrait à la rigueur ne pas insister auprès des autres officiers pour qu'ils se mettent au courant d'une partie de la science militaire qui serait régulièrement aux mains d'un personnel spécial. Mais actuellement les ateliers de chiffrement des corps de troupe ne sont constitués que d'éléments de fortune, et les chefs de ces ateliers de guerre, qui seront vraisemblablement des officiers de réserve, n'ont reçu de professeurs qualifiés aucune indication sur leur rôle. D'autre part, la conversation téléphonique (bien qu'en règle générale l'emploi du message téléphoné, rédigé comme un télégramme et transmis par le personnel des transmissions soit réglementaire, et facilite l'usage des messages chiffrés) est tellement généralisée dans la pratique qu'elle risque d'entraîner des chiffrements en des points particulièrement reconnus comme dangereux et où il n'y a pas de chiffreurs spécialistes ; l'officier présent devra chiffrer. Enfin il est nécessaire que le commandement sache ce qu'il peut demander comme communications chiffrées et ce qui dépasse la capacité des moyens mis à sa disposition. Il est donc utile que l'on vous parle du chiffrement dans les petites unités. Cela va former le sujet de la troisième partie de cette conférence.

Je vous ai dit que les documents de *chiffrement réglementaires* chez nous étaient du type dictionnaire, et qu'ils étaient plus ou moins riches suivant l'autorité qui en disposait. Pour des facilités de langage, on a donné des noms différents aux documents de l'armée, suivant leur richesse, et on a ainsi le dictionnaire chiffré des corps d'armée, en groupes de *5 chiffres;* le code avec des groupes de *4 chiffres* qui est le document imprimé dont disposent les état-majors de divisions, d'I. D., d'A. D., les commandants de régiments, de groupes d'artillerie et d'une façon générale tous les commandants d'une unité pouvant recevoir directement des ordres de la division ; enfin, à l'intérieur des corps de troupe, le carnet de chiffre, en groupe de 3 chiffres. Le code est, en principe, un document unique pour tout le front, et permet à une unité changeant de secteur de communiquer avec le nouveau commandement dès son arrivée. Le carnet varie d'un secteur à l'autre. Bien entendu, les unités supérieures ont les documents des unités inférieures ; un cryptogramme chiffré avec le carnet peut être déchiffré au corps d'armée, et ne doit, sous aucun prétexte, être par exemple rechiffré en code à l'Etat-major du régiment. Remarquons qu'au cours d'une action les postes T. S. F. des unités supérieures entendent une partie des messages qu'échangent entre elles les unités inférieures. Le commandement est renseigné immédiatement, par leur traduction, sans attendre des comptes rendus qui deviennent inutiles.

Les documents que nous avons énumérés, en particulier le

code et le carnet qui nous intéressent plus particulièrement, ne sont pas sortis sous leur forme actuelle du cerveau d'un spécialiste. A ce propos quelques mots d'histoire ne seront pas superflus. Au début de la guerre, on ne pensait pas à chiffrer au téléphone, et comme seuls les Etats-majors d'armée avaient la T. S. F., on n'avait pas donné de moyen de chiffrement aux corp de troupe, sauf à la cavalerie. Les Etats-majors ne disposaient d'ailleurs que de procédés cryptographiques littéraux. Nos postes de T. S. F. restèrent d'abord muets ou à peu près, car se rendant compte des dangers de ce genre de communication, et disposant du réseau télégraphique du territoire national, le G. Q. G. donna dès les premiers jours de son existence l'ordre de n'utiliser la T. S. F. qu'en cas de nécessité absolue, à défaut de tout autre procédé de transmission. Les postes allemands, par contre, parlèrent beaucoup en *août*, *septembre* et *octobre* 1914 ; l'emploi de la *radiotélégraphie* était *élégant* et *scientifique*, ce qui plait à l'Allemand, et on opérait en pays ennemi où le fil télégraphique était détruit. Mais, les *cryptologues français* ayant réussi à partir du 1er octobre à traduire les télégrammes allemands, et la presse ayant divulgué ce résultat, les Allemands, lors de la *stabilisation*, renoncèrent aussi à l'emploi de la T. S. F.

C'est que la T. S. F. présente au point de vue militaire des dangers graves et nombreux. Chaque armée a des postes d'écoute, chargés de recueillir les communications ennemies et de les remettre à un service de spécialistes qui cherche à les traduire. Ces spécialistes ont intérêt, comme je vous l'ai expliqué à propos des mots syllabés dont les répétitions sont d'autant plus nombreuses en général qu'on dispose de plus de textes, à avoir le plus grand nombre possible d'éléments d'étude. Tout emploi de la T. S. F. multiplie les textes et favorise les cryptologues. D'autre part, si l'on admet que les grandes unités mettent en action un nombre donné d'appareils, l'augmentation ou la diminution du nombre de postes en service sur un front indique le renforcement ou la réduction de la densité de ce front. Le changement de place des postes donne des indices sur des mouvements de troupe. Or, on a des procédés qui permettent de déterminer la situation des postes sur le terrain et de voir s'ils en changent. Cette situation intéresse non seulement les officiers chargés d'étudier l'ordre de bataille ennemi, mais tout particulièrement le *cryptologue*. Celui-ci, lorsque l'ennemi utilise des documents différents d'un secteur à l'autre, ne doit pas mélanger dans ses études les textes chiffrés au moyen d'un code avec les textes chiffrés au moyen d'un autre. Généralement, en réunissant les correspondances de deux postes donnés entre eux, on a des chances, à cause des nécessités de service qui empêchent des changements trop fréquents, d'avoir des textes de même nature. Les postes s'avertissent de l'envoi d'un message

en s'appelant par des groupes de lettres qu'on appelle indicatifs, et qui sont alors la caractéristique du poste. Au début de la guerre, les indicatifs changeaient rarement, et en groupant les textes portant des indicatifs donnés, on pouvait espérer travailler sur un dossier homogène. Pour dérouter l'ennemi, on changea dans la suite fréquemment les indicatifs des postes et on alla jusqu'à les modifier tous les jours. Les indicatifs ne suffisent plus alors à identifier les postes pour une période de plusieurs journées ; il faut se rapporter à la situation sur le terrain. L'emploi des appareils qui permettent la détermination de cet emplacement étant facilité par la transmission de messages nombreux et longs, on aura intérêt pour compliquer la tâche de l'ennemi à ne passer que des messages aussi rares et aussi brefs que possible. Ainsi l'emploi, et surtout l'abus, de la T. S. F. favorise pour plusieurs motifs les services de renseignements ennemis.

Après cette digression, reprenons l'historique abrégé de l'emploi de la T. S. F. et du *chiffre*.

Comme l'attribution des postes de T. S. F. à terre n'était pas encore descendue au-dessous des états-majors des grandes unités, les émissions d'avions furent, au cours de l'année 1915, les seules que purent recueillir les postes d'écoute du front. On avait adopté chez nous, pour permettre aux aviateurs de faire part de leurs découvertes, sans expédier de trop longs messages dont leur situation à bord rendait l'émission difficile, une liste d'abréviations en *3 lettres*, où ART signifiait *artillerie*, AMI, *ami*, PCT, *poste de commandement*, etc..., et les messages de T. S. F. étaient composés de groupes de ce genre.

En février 1916, le *général Dubail*, commandant l'armée de Lorraine, s'aperçut que certaines relèves étaient particulièrment canonnées, et, des postes spéciaux d'écoute téléphonique étant installés sur son front, il put constater d'une part que ces relèves étaient celles qui donnaient lieu à des conversations téléphoniques longues et précises que les postes spéciaux ennemis pouvaient entendre, de l'autre que les Allemands chiffraient une partie de leurs conversations téléphoniques. Il demanda alors l'établissement d'un document de chiffre à utiliser pour le téléphone et on établit un premier type de carnet. Lorsque, peu après on commença à distribuer dans les corps de troupes des postes de T. S. F., *émetteurs* et non *récepteurs*, permettant seulement de signaler à *l'arrière* ce qui se passait à *l'avant*, on hésita quelque temps sur le moyen de correspondance à donner à ces postes. On commença par leur interdire les communications en clair. Puis, comme ils étaient du genre des postes d'avions, on leur imposa l'emploi exclusif de la liste des groupes en 3 lettres des abréviations d'avion. Enfin, sur la demande expresse des détenteurs de postes, qui trouvaient trop limité ce moyen

de correspondance, on modifia le carnet établi pour le téléphone afin d'en étendre l'usage à la T. S. F. Dans la suite, l'attribution de postes de T. S. F. à des unités de plus en plus nombreuses et la création d'un réseau de division amena le développement de la richesse du carnet. Puis, pour ne pas confier aux éléments de première ligne un document volumineux dont l'établissement présentait des difficultés, on le scinda pour former les deux documents qui sont maintenant le code et le carnet.

C'est donc sur la demande des combattants que ce matériel a été créé. C'est en étroite collaboration avec eux qu'a été établie la liste des mots et des expressions qui y figurent. C'est aussi sur la demande des exécutants, qui préféraient, avec le personnel parfaitement exercé de 1917, passer au télégraphe des groupes de lettres plutôt que des groupes de chiffres composés de signaux Morse plus longs, qu'on a adopté, après divers essais, l'opération de transformation des chiffres en lettres qui, rendue indispensable pour la sécurité comme on le vit par la lecture de documents allemands, constitue maintenant le surchiffrement. On doit remarquer que les unités présentes au front écrivaient fréquemment pour se plaindre des négligences de chiffrement de leurs voisines et demander une aggravation des consignes ainsi qu'une nouvelle complication des procédés, tandis qu'une fois au repos elles déclaraient généralement inutiles les précautions nouvelles rendues réglementaires.

Maintenant nos unités sont au repos, et le chiffrement avec les complications qu'entraîne le surchiffrement a une presse déplorable dans l'armée française. Comme les gens qui ont acquis l'expérience du chiffre pendant la guerre sont très rares, chacun en parle *a priori*, avec son imagination. « Il est évident que...» est une phrase que nous entendons souvent quand on nous demande des modifications au chiffre. Au début de 1914, il était non moins évident pour bien des gens qui n'avaient pas creusé le sens profond des règlements, qu'une course rapide à travers champs vers l'ennemi, dénommée par ces imaginatifs « *offensive* », nous donnerait la victoire : l'expérience de ceux qui avaient étudié la question répondait : « Gare au feu. » Maintenant nous disons : « Gare aux renseignements que, faute de chiffrer, vous donnerez à l'ennemi. »

Les reproches qu'on fait ordinairement au chiffre et les objections à l'emploi des procédés réglementaires se ramènent à ceci : la pratique du chiffrement retarde les communications et empêche les procédés scientifiques modernes de transmission d'avoir leur plein rendement. Et les modalités de ces objections sont entre autres : pourquoi vous opposez-vous aux communications par T. S. F. en clair qui ordinairement n'apprennent rien à l'ennemi ? Pourquoi imposez-vous le surchiffrement ? Puis un grand axiome souvent répété : On ne chiffre pas sous le

feu, le carnet de chiffre est inutile, on peut trouver des moyens de communication bien plus simples et suffisamment sûrs.

Reprenons ces arguments. Les règlements interdisent en principe les communications en clair lorsqu'elles peuvent être interceptées par l'ennemi. C'est que les officiers qui ont été dans les services de renseignements savent qu'une information insignifiante, qui paraît innocente à son auteur, prend parfois, par rapprochement avec d'autres, une importance de premier ordre. Le commandant d'artillerie, qui, en 1918, prescrivait que les dépôts de munitions soient au complet pour une date donnée du début de juin, ne se doutait pas qu'il allait orienter vers *Montdidier* les divisions tenues en réserve à mi-chemin de *Châlons* et de la *Somme*, dans l'incertitude où se trouvait le commandement sur la partie du front que menaçait l'attaque à laquelle on s'attendait, et que ces divisions placées sous les ordres du général *Mangin* allaient arrêter à *Méry* la progression allemande vers Compiègne. Les télégrammes en clair de la cavalerie allemande de *von Marwitz*, en fin août 1914, donnèrent par des demandes de ferrure, de ravitaillement, etc..., des renseignements sur l'état matériel de l'armée allemande qui révélaient un certain désordre et ne furent peut-être pas sans influence sur la date de la reprise de notre offensive. On trouve enfin dans une notice sur l'emploi du chiffrement dans les petites unités, éditée à la date du 1er juillet 1924 par l'Etat-major de l'armée, des exemples qui montrent les conséquences de conversations en clair qui auraient dû être chiffrées, et même de l'intérêt que les Allemands prenaient aux communications en clair, et aussi d'ailleurs en chiffres, de nos avions de réglage.

Nous ajouterons, dans cette réponse à la première objection mentionnée, qu'on nous dit parfois : Au moment du combat l'ennemi a bien autre chose à faire que d'écouter vos conversations. C'est oublier complètement les résultats de la spécialisation du personnel et de la répartition du travail. Au moment du combat les fantassins progressent, les artilleurs tirent, les aviateurs volent, les écouteurs, dans leurs trous sous terre ou à leur antennes à l'arrière, écoutent, et les *décrypteurs* dans leurs bureaux *décryptent*. Peut-être dira-t-on que les renseignements recueillis seront sans utilité étant donnée la rapidité avec laquelle se déroulent les événements ; c'est possible, mais ce n'est pas sûr, et justement parce qu'il y a des événements qui peuvent faire le sujet de messages, ceux-ci pourront être très utiles au point de vue cryptographique pour fournir des hypothèses sur les noms syllabés par exemple.

Le règlement permet d'ailleurs au commandement de donner, en connaissance de cause, l'ordre de passer des radio-messages en clair. C'est ce qui fut fait lors de l'affaire de Méry mentionnée plus haut, où les divisions mises en ligne n'avaient pas les mêmes documents. Ce qui est interdit rigoureusement,

c'est le mélange du chiffre au clair, les mots en clair permettant de deviner le sens des groupes. Dans un message : Nous avons vingt-cinq blessés 492 et huit 536, on devine facilement 492 légers et 536 graves.

Pourquoi impose-t-on le *surchiffrement*, et ne permet-on pas l'emploi du chiffrement *simple* ? Ce que je vous ai dit à propos des dictionnaires et du danger des répétitions l'explique. Des documents allemands nous ont appris que nos messages non surchiffrés avaient été traduits. Mais, dit-on encore, on ne surchiffrera pas, et même en on chiffrera pas, sous le feu. Le carnet, par suite, est inutile. Nous reviendrons sur l'argument du feu. Mais, en déclarant le carnet inutile, il fallait assurer les communications, même sous le feu. Avant d'exposer les dispositions à ce sujet, disons encore un mot du carnet.

Je n'examinerai point ici, sa contexture. Le type actuel n'est point immuable. On a en vue des modifications qui seront peut être des améliorations. Mais, tandis que les questions budgétaires nous interdisent les changements trop fréquents, il est de bonne guerre, en chiffre, de ne pas trop tôt démasquer ses batteries et de ne pas mettre en circulation des documents du type mobilisation. Le carnet actuel est un bon document d'instruction. Je n'insisterai pas à nouveau sur les précautions à prendre dans son emploi, j'en ai parlé plus haut dans les généralités : éviter les répétitions est la précaution principale. Le carnet d'instruction est du reste encarté dans un document où les mesures de précautions sont énumérées et commentées, la Notice sur les procédés de chiffrement dans les petites unités du 1er juillet 1924. Toutes les consignes de précautions qui y sont énumérées, quelque ennuyeuses et inutiles qu'elles paraissent à certains, sont des résultats de l'expérience des décrypteurs. Aucune n'a été imposée *a priori* sans que des exemples puissent être donnés à l'appui de sa nécessité.

En dehors des règles d'emploi du carnet, la notice du 1er juillet 1924 traite d'autres questions, relatives aux moyens de communication autres que le carnet. Voici pourquoi : Après la guerre, quand on voulut réorganiser l'instruction du chiffre, on s'aperçut que les corps de troupe n'avaient aucun guide dans ce domaine. D'autre part, l'instruction provisoire du 26 mai 1926 sur l'organisation et le fonctionnement de la liaison et des transmissions mentionnait un certain nombre de procédés de communication rapide mis à la disposition des corps de troupes, mais sans trop préciser les conditions de leur emploi. L'Etat-major de l'armée établit alors, en même temps qu'un nouveau carnet de chiffre destiné à l'instruction, la notice dont il s'agit, où l'on rappelle, à propos des procédés de transmission dont disposent les unités, les précautions à prendre pour la sécurité et les règles à suivre pour la rapidité des communications.

On semble admettre implicitement une certaine classifica-

tion des catégories de communications qui intéressent les petites unités : d'abord les communications au cours de la bataille, demandes de tir, de ravitaillement, etc... de première importance pour l'existence immédiate des unités et l'accomplissement de leur mission ; puis les communications de renseignements, soit pendant le combat, soit en dehors de lui, demandes diverses, encore importantes sans doute, mais pouvant donner lieu à une entente ou une conversation, tandis que la première catégorie doit recevoir satisfaction immédiate sans discussion ; enfin communications de la vie courante des unités, surtout en dehors de la bataille, ou du moins pendant les accalmies.

Pour les premières, on a adopté des signaux. Souvent elles ont correspondu avant l'emploi de la T. S. F., et correspondent encore, à des combinaisons de fusées ou de panneaux, et la T. S. F. n'a à remplir qu'un rôle analogue, en émettant des signaux brefs, quelques traits et quelques points, ayant une signification connue de tous, séries de trois traits pour un tir de barrage, de trois points quand on reçoit des coups de sa propre artillerie, etc... L'ensemble des combinaisons de cette sorte, forme « la signalisation », qui, semble-t-il et répète-t-on, doit être suffisante pour les besoins des troupes engagées dans une attaque.

Pour les secondes, on a utilisé ces abréviations qu'on avait tout d'abord données aux avions pour communiquer avec la terre : ART artillerie, PCT poste de commandement, etc... Au lieu de désigner cet ensemble de combinaisons de lettres par le mot d'abréviations, on l'a appelé « *code de condensation* », et les messages qui utilisent ce code sont dits *messages condensés*. On peut en réunissant plusieurs de ces groupes de condensation faire des phrases très simples, bien que l'absence de verbes et de propositions soit fort gênante pour cet objet, et que le langage genre « *langage nègre* » prête souvent à ambiguïté. Toutefois ces expressions, créées pour l'avion qui voit loin, sont peu commodes pour le fantassin à terre. Comme on a voulu pendant la guerre généraliser l'emploi de ce moyen de correspondance, qui permet de raccourcir les messages, et qu'on a craint de renseigner l'ennemi en employant toujours les mêmes groupes de lettres, on a prescrit, en 1917, que chaque armée établirait une liste de ces signaux en les chiffrant, c'est-à-dire en les transformant en groupes de 4 lettres, commençant tous par la même lettre pour qu'on reconnaisse tout de suite à quel type de document on a affaire. Cette liste, différente d'une armée à l'autre, devait être fréquemment changée, avant, espérait-on, que l'ennemi ait pu comprendre le sens des signaux en les comparant aux événements. La condensation use donc de groupes de trois lettres, quand on considère le message comme clair, et de groupe de quatre, pour un chiffrement déclaré obligatoire chaque fois qu'on donne un renseignement sur les trou-

pes amies. Dans les communications de cette nature on a souvent besoin de désigner un emplacement par les coordonnées qui le situent par rapport à un quadrillage porté sur les cartes. On chiffre ces coordonnées en remplaçant les chiffres par des lettres, au moyen d'un mot clef de *10 lettres* différentes, la première *chiffrant 1 la seconde 2,* etc... Exemple : clef LE GROS CHAT, 3482 est remplacé par GRHE.

Enfin comme, malgré les théories actuelles qui veulent réduire à la signalisation et à la condensation, ainsi qu'on a tenté en vain de le faire en 1916, les moyens mis à la disposition de la T. S. F. et de la T. P. S. des corps de troupe, ces deux procédés ont été déclarés très insuffisants pendant la guerre, on a, pour faire des phrases sur n'importe quel sujet, recours au carnet de chiffre, dont l'emploi, même s'il est difficile pendant la bataille, sera normal pendant les périodes de marche et de stabilisation.

Sans attacher une importance exagérée à l'argument « on ne chiffre pas *sous le feu* », car nous considérons que, « *sous le feu* » on ne fait rien, en effet, pas même d'étaler les panneaux de jalonement, et que dans les accalmies qui durent parfois des heures, l'état-major d'un bataillon peut parfaitement chiffrer, on doit toutefois reconnaître que les messages faits avec le carnet sont parfois longs à chiffrer et à transmettre, car le carnet n'est pas riche et il faut beaucoup chiffrer par syllabes. C'est là un défaut. La condensation n'est pas d'autre part, comme nous l'avons dit, fort commode pour les troupes à terre avec sa liste actuelle, et on ne peut, pour des raisons matérielles qui feraient d'une trop longue liste un document analogue au carnet, développer cette liste à l'excès. On a alors imaginé de simplifier l'emploi de ces deux procédés par la création d'un document nouveau qu'on a appelé le *plan de chiffrement.*

Ce qui gêne dans l'emploi de la condensation, qui, nous le rappelons, est le procédé de l'aviateur et ne doit pas constituer un document encombrant, c'est qu'on ne peut étendre indéfiniment le tableau pour y mettre des expressions nouvelles. Ce qui gêne avec le carnet, c'est que dans certaines situations on a besoin de mots qui ne s'y trouvent pas. Eh bien, on peut établir, dans les circonstances où l'on peut prévoir qu'on aura certaines choses à dire, un tableau de chiffrement spécial, temporaire, où l'unité qui aura une opération à exécuter par exemple, fera figurer les mots, et surtout les phrases, dont elle croit avoir besoin. On représentera ces mots et ces phrases par des groupes puisés dans un approvisionnement, réglé par l'autorité supérieure de manière à éviter les doubles emplois d'un groupe dans deux unités voisines et les incertitudes et les contre-sens qui pourraient en résulter.

Dans ce *plan de chiffrement,* on fera figurer, pour les

représenter par un seul groupe, les mots qui ne se trouvent pas dans les documents préparés longtemps à l'avance, signalisation, condensation ou carnet. Au premier rang seront les noms propres. On leur donnera des noms nouveaux, soit à employer tels quels pour la condensation, soit quand on les introduira dans les messages faits avec le carnet, courts à chiffrer, ne donnant pas lieu à ces répétitions de séries de groupes que nous avons signalées comme si dangereuses pour les codes. COLOMBES-LES-DEUX-EGLISES deviendra par exemple BARI. On agira de même avec les désignations d'unités, qui donnent lieu aussi à des séries de groupes, et qui furent un des clous où s'accrochèrent des déchiffrements des carnets allemands en 1917 et 1918. Ces deux sortes d'éléments pourront être l'objet de listes établies pour quelques jours à l'échelon supérieur : nous disons pour quelques jours, parce que, quand on ne surchiffre pas, il faut changer souvent le tableau de chiffrement. Mais en dehors de cette partie qui forme le canevas du plan, la grande unité ne doit pas, à notre avis, chercher à trop étendre les phrases dont elle croit l'emploi à prévoir, parce qu'elle ne peut préparer la traduction de tous les événements précis du front qu'avec un document énorme, et que si elle reste dans les généralités, elle ne fera que doubler le carnet où se trouvent déjà une centaine de phrases toutes faites. C'est donc à chaque élément qui va s'engager dans une action, et qui prépare son plan d'engagement, son plan de feux, son plan de ravitaillement, en vue de l'opération *déterminée* qu'il va entreprendre, qu'il appartient de préparer aussi son plan de chiffrement, c'est-à-dire la convention des signaux à transmettre pour correspondre. Ainsi le capitaine qui va faire un coup de main s'entendra avec son chef ; si l'ouvrage ennemi bombardé est vide, je vous ferai faire le signal KAPT. S'il faut recommencer le bombardement KLIZ. Si les abris sont encore occupés et que j'aie besoin de renforts KMFR. Si la tranchée à contre-pente est occupée, je vous demanderai un tir d'artillerie sur la gauche par KBSF, sur la droite par KOBI, et ainsi de suite. J'ai étudié ainsi dans un corps de troupe la liaison infanterie-artillerie, non pas sur des thèmes généraux avec des prescriptions vagues, mais sur les cas concrets successifs que pose sur le terrain chaque progression du combat, avec des plans de chiffrement également successifs établis par l'officier de liaison et, une fois le personnel instruit, la liaison a très convenablement marché avec de simples signaleurs à bras, sans attente pour la pose des lignes téléphoniques, sans T. S. F. ni T. P. S.

Pour les opérations prévues à l'avance, pour les renseignements courants de secteur, pour certains modes de liaison chers à telle ou telle unité, c'est avec de tels plans de chiffrement établis à mesure que se déroulent les événements qu'on obtiendra le mieux le résultat désirable, en tenant compte des inconvé-

nients de la T. S. F. et du nombre d'appareils capables d'être mis en jeu dans un secteur étroit où ils risquent de se gêner mutuellement, à savoir assurer les liaisons par des émissions aussi brèves que possible. Sans doute, le carnet reste pour chiffrer les textes se rapportant à des événements imprévus, comme il s'en produit toujours à la guerre, mais des officiers spécialisés dans les fonctions du chiffre, habitués à la forme des ordres de leurs chefs, à leur manière de conduire le combat, faisant partie de l'entourage de ces chefs et par suite connaissant leurs projets pour la première période de temps qui va s'écouler, habiles à préparer ensuite un document nouveau pour une situation nouvelle, arriveront à donner aux liaisons avec des conventions de chiffrement, ou de condensation (le mot ne fait rien à la chose) du moment, une souplesse inconnue actuellement dans les exercices et que les documents préparés d'avance sont incapables d'assurer.

Mais l'emploi de ces divers procédés, *signalisation, condensation, plan de chiffrement, carnet*, et même *code* avec les échelons supérieurs, exige une instruction préalable. Cette instruction n'est pas bien compliquée. En quelques séances, six à huit heures en tout, la section du chiffre se chargerait du dressage de chefs d'ateliers très suffisants, même au début d'une campagne où les flottements sont impossibles à éviter. tant dans le service de transmissions que dans les autres. Mais, tandis qu'on s'occupe de dresser, si possible, des T. S. F. istes, des téléphonistes, des signaleurs à bras, etc., c'est-à-dire des transmetteurs, nul ne semble s'occuper avec compétence de dresser les gens qui auront à établir les messages à transmettre. Il a fallu une certaine période, disent les employés du télégraphe, pour apprendre à une partie du public à rédiger des télégrammes d'affaires, explicites et limités. Il faudra une période également pour apprendre aux militaires à utiliser convenablement les procédés mécaniques de transmission. Enfin, pour que le spécialiste du chiffre d'un régiment, le collègue du spécialiste des transmissions (car les deux rôles seraient lourds pour un même personnage, surtout si le second exigeait un déplacement pour parer à un accroc) puisse assurer sa tâche dans de bonnes conditions, il faut que tout le monde connaisse en gros les bases de son service, et ne lui donne pas à transmettre de discours à l'Académie, ni des textes inutiles qui embouteillent le réseau des transmissions. Comme je l'ai dit il ne faut utiliser la T. S. F. qu'à défaut de tout autre procédé, les instructions allemandes et françaises de la fin de la guerre sont d'accord sur ce point, ainsi que l'instruction provisoire actuelle sur la liaison et les transmissions, au paragraphe : Défense technique contre les recherches ennemies. Il faut n'utiliser un réseau de transmissions de corps de troupe, dont le débit est limité, qu'à bon escient, et lorsque pendant la guerre des réseaux de division

passaient trois fois par jour pendant une semaine la phrase chiffrée « *Secteur calme, rien à signaler* », c'était un abus fort net de la T. S. F., qui non seulement permettait à l'ennemi d'être sûr que le secteur n'était pas modifié, mais encore lui facilitait la traduction des nouveaux documents mis en service.

Je m'en tiendrai, en ce qui concerne l'emploi du *chiffrement* et des autres moyens de rédaction des messages, à ces notions élémentaires. Mais, à propos de chiffre, il est encore un point nécessaire à traiter.

Je vous ai dit qu'un des moyens commodes de traduire les correspondances étrangères étaient la possession du dictionnaire ou tout au moins de documents en clair dont on possède le texte chiffré. Il arrive à la guerre que sur le terrain on trouve des codes de chiffrement ennemis ou des ordres provenant de déchiffrements et que dans les carnets d'officiers on trouve des renseignements sur le chiffrement. J'ai découvert en 1918, dans les bagages d'un hôpital, des documents qui auraient été fort précieux pour le chiffre en 1916, et qu'un homme avait conservés « comme souvenir » sans en soupçonner la valeur. Puis-je vous rappeler ici que la transmission rapide de tous les éléments pouvant donner des renseignements sur l'ennemi est un des devoirs de tous à la guerre. En 1918 encore, j'ai vu dévaster des P. C. ennemis par les premières troupes qui y pénétraient. Tous, officiers en tête, rivalisaient pour jeter dans la boue, après un semblant d'examen, les documents que dans sa hâte l'ennemi y avait laissés. Là encore, il y avait grave faute militaire. Par la difficulté de sa tâche, le service du *chiffre* est un des plus intéressés dans l'examen des documents conquis. Le cas échéant, j'espère que vous voudrez bien vous en souvenir.

Je termine ici cette conférence déjà longue. Je voudrais que vous en reteniez les points suivants : en chiffre comme dans n'importe quel métier, il faut avoir appris pour savoir, les improvisations ne valent en général rien. Le chiffre est un serviteur très sensible aux mauvais traitements : si l'on chiffre mal, on laisse traduire sa correspondance, et, ce qui est plus grave, la correspondance des voisins qui ont les mêmes documents. Enfin, même en admettant que le service des transmissions fonctionne admirablement, il y a des précautions à prendre, en particulier celle de ne l'utiliser qu'à bon escient, pour éviter d'abord d'embouteiller le réseau et d'arrêter pour des conversations au moins inutiles des communications urgentes, et puis parce que l'ennemi vous écoute, que des incidents de transmission peuvent sur des circuits que vous croyez sûrs transformer cette phrase en celle-ci : L'ennemi vous entend, et que des communications qui vous semblent anodines peuvent, par des recoupements, devenir de dangereuses machines de

guerre. Il y a des consignes de transmissions, il est urgent de les respecter. Souvent on a négligé de le faire pendant les dernières campagnes, l'attention n'ayant pas été préalablement attirée sur ces points et les instructions faites en cours de la guerre étant souvent adressées à un personnel qui croyait savoir et ne voulait plus qu'on tente de l'instruire. Les dernières manœuvres ont montré qu'actuellement encore tout ce domaine des transmissions et du chiffre est bien mal connu de la plupart des officiers. Puissé-je avoir jeté dans vos esprits la semence qui germerait le cas échéant, et vous éviterait des imprudences funestes pour vous et pour vos camarades.

Imprimerie F. ESSERTIER
8, impasse du Maine, Paris