GOUVERNEMENT MILITAIRE DE PARIS

SIÈGE SOCIAL :
83, Boulevard de l'Hôpital
PARIS (13e)

Chèques postaux : 505-08

ECOLE d'INSTRUCTION
de la 7e D. I.

CONFÉRENCE
publiée par les soins de
l'Association des Officiers de Complément
de l'Ecole d'Instruction d'Infanterie
de l'Ecole Militaire, Paris
Fondée le 24 Avril 1907

(Déclaration nº 152-611)

ANNÉE 1922-23

QUESTIONS de CHIFFRE

CONFÉRENCE

faite le 28 Janvier 1923

aux Officiers de Complément de toutes armes
du Gouvernement Militaire de Paris

par UN OFFICIER

de la Section du Chiffre de l'Etat-Major de l'Armée

QUESTIONS DE CHIFFRE

CONFÉRENCE FAITE

aux Officiers de Complément de toutes armes du Gouvernement Militaire de Paris

par UN OFFICIER

de la Section du Chiffre de l'Etat-Major de l'Armée

Messieurs,

Les communications des éléments avancés avec les chefs dont il dépendaient, les transmissions des renseignements de la ligne de combat à l'artillerie ou aux réserves, ont constitué des problèmes considérés comme des plus graves parmi ceux qui ont pris naissance au cours de la dernière guerre. Les coureurs ont eu à traverser des terrains rendus impraticables par le feu, les fils de fer, les obstacles de toute sorte créés par les bombardements. Les câbles téléphoniques, les nappes, ont été fréquemment rompus, et l'entretien de ces fils au moment du combat a coûté de nombreuses vies humaines sans assurer un bon service. Les fusées ont donné lieu à de graves erreurs d'interprétation. Une des meilleures solutions a été fournie par la T. S. F. et la T. P. S., qui, dans la période de stabilisation, ont donné des résultats satisfaisants, encore que dans les journées de progression on n'ait pas toujours réussi à garder les appareils au contact des troupes. Dans l'avenir, l'emploi de chars portant des postes d'émission permet d'escompter un contact permanent. L'emploi des radio-messages à l'avant paraît donc devoir constituer une des caractéristiques des prochaines guerres.

A l'arrière, la menace que fera peser l'aviation ennemie sur les grandes artères télégraphiques, qui suivent les routes et les chemins de fer, rend également probable l'emploi de la T. S. F. plus encore que dans la dernière guerre. Il n'est donc pas aventuré de dire que les ondes transmettant les radio-télégrammes devront couvrir la zone des armées et sans doute même tout le pays, peut-être la terre entière. Or dans les conditions actuelles de la T. S. F,.

de telles ondes peuvent être captées par tout indiscret, par l'ennemi sur le front, par les neutres plus ou moins bienveillants et par l'ennemi lui-même pour les communications à longue portée dirigées même à l'inverse des théâtres d'opérations. Si les messages sont transmis sous une forme qui n'en dissimule point le sens, les renseignements confiés à la radiotélégraphie sont par cela même rendus publics. Cela peut être fort gênant dans certains cas.

Pour cacher le sens de ces messages on a recours au chiffre.

Le chiffre, tant qu'on n'aura pas le moyen d'empêcher un autre individu que le destinataire d'un radiogramme de capter le texte de ce dernier est indispensable pour assurer le secret des communications et, aussi bien que dans les ministères et dans les états-majors, on doit chiffrer dans toutes les unités militaires où l'on a à communiquer par la T. S. F. des renseignements qui doivent rester secrets.

Le service du chiffre a donc, parmi ses attributions, celle d'assurer la dissimulation du sens d'un message. Un bureau central, permanent, s'occupe d'examiner les différents systèmes et procédés qui peuvent être employés dans ce but et d'en assurer la connaissance parmi ceux qui doivent l'utiliser. Les procédés règlementaires sont changés de temps en temps, pour des motifs que vous comprendrez au cours de cette conférence. Actuellement, ils diffèrent suivant la catégorie dans laquelle peuvent être rangés les correspondants, au point de vue des distances à parcourir, des appareils de transmission et de l'importance des sujets traités dans les messages.

Nous n'insisterons pas sur les procédés de chiffrement réservés aux échelons supérieurs. Nous essaierons, dans la présente conférence, de vous indiquer quels sont les documents que les régiments, bataillons et organes inférieurs auront à leur disposition pour chiffrer, l'emploi à faire de ces documents, et les précautions à prendre pour que le secret des communications ne soit pas trop aventuré.

Les ouvrages de cryptographie classent les méthodes de chiffrement, c'est-à-dire les moyens dont on dispose pour cacher le contenu d'un texte, en méthodes alphabétiques et méthodes à répertoire ou à dictionnaire. Nous ne considérerons que les procédés qui donnent lieu à des cryptogrammes transmissibles par télégraphe, à fil ou sans fil, en respectant les conventions télégraphiques, et ceci nous oblige à ne passer des messages qu'en lettres ou en chiffres figurant sur nos appareils. Dans les méthodes alphabétiques, on fait subir aux lettres du texte diverses modifications, portant soit sur l'ordre des lettres dans la phrase, soit sur le nom des lettres qu'on remplace par d'autres lettres ou par des groupes de chiffres. Nous n'insisterons pas, car, actuellement, des procédés de ce genre ne sont pas règlementaires pour la correspondance qui nous inté-

resse. Dans les procédés à répertoire, les correspondants ont eu leur possession des listes de mots ou d'expressions, où chaque ligne portant un mot ou une expression est numérotée, si bien que la communication du numéro de la ligne indique sans erreur ni ambiguité possible le mot ou l'expression correspondant. Si seuls les intéressés possèdent des listes, leur correspondance est secrète, puisque la T. S. F. ne transmet que des numéros de lignes ; si un tiers se procure un tableau, à la suite d'une imprudence d'un des possesseurs, ou parvient à reconstituer l'équivalence des mots et des numéros de ligne, il peut traduire les messages et le secret est brûlé.

Afin de se garantir dans une certaine mesure contre ce danger, on peut changer assez souvent la liste ou le code. Si l'ennemi n'a pas un espion fournisseur régulier, il aura des difficultés à se procurer un exemplaire du nouveau document, ou à le reconstituer. On peut aussi, et c'est ce qui a été fait pendant la dernière guerre, compartimenter un front étendu en donnant à chaque secteur un code différent, si bien que la connaissance du code employé en Lorraine ne trahira pas le secret des opérations en Champagne, mais cela devient gênant au cas où des troupes sont amenées rapidement d'un secteur dans l'autre, parce qu'elles n'ont pas dès leur arrivée le même code que leurs nouveaux voisins. Quel que soit le procédé employé, les remplacements de codes sont des opérations assez délicates, sans compter qu'elles sont coûteuses, et il est du devoir de tous d'éviter d'en augmenter la nécessité. Or, pendant la dernière guerre, on a trop souvent négligé toute précaution à cet égard.

Pourtant des instructions nombreuses avaient dû être faites Les premiers codes distribués portaient en tête des conseils pour chiffrer précédés de la phrase : « Prière de les lire. ». Trop souvent ils n'ont point été lus, ou n'ont point été compris, et c'est pour remplacer la lecture d'instruction par des explications verbales que l'on a décidé de faire cette Conférence. Je traiterai tout d'abord de certaines imprudences matérielles, constamment renouvelées, que chacun trouve absolument inouies en attendant qu'il en fasse d'équivalentes. Il ne faut point emporter les codes en reconnaissance, où l'on court le risque d'être tué ou pris, et où l'on n'a pas besoin de codes puisqu'on n'a pas de T. S. F. Il ne faut pas les laisser traîner sans surveillance, parce qu'un homme qui a envie de déserter les emportera pour se faire bien voir de l'ennemi. Il ne faut pas, en cas d'attaque ennemie qui semble progresser, attendre trop longtemps pour détruire le code ou l'enterrer afin d'empêcher qu'il soit pris. Il ne faut pas, quand un code est remplacé par un autre, négliger de rendre le premier sous prétexte qu'il n'est plus utiles et le laisser dans un P. C. où un coup de main de l'ennemi le fera prendre, ce qui permettra de lire la correspondance des jours écoulés, et d'y trouver des renseignements sur les approvisionnements et les effectifs.

Mais ce sont là des imprudences matérielles qui ne constituent qu'une part du profond et déplorable mépris qu'ont beaucoup de français pour les précautions touchant le secret des opérations de guerre : Taisez-vous ! Méfiez-vous !

En dehors de cela, il y a des imprudences techniques, et, avant de vous en parler, je vais vous dire quelques mots d'une science fort spéciale, qui a rendu pendant la guerre de grands services : c'est la science du décryptement. Elle comprend les recherches faites sur les documents chiffrés dont on n'a pas la clef, en vue de trouver cette clef et de traduire les cryptogrammes. Dans la Revue militaire du 1er juillet 1921, on trouve cette information, sous la plume du général Dupont qui fut chef du 2e Bureau du G. Q. G. :

« On connaît la manœuvre qui amena la victoire de Tannenberg à la fin d'août, Ludendorff la raconte tout au long dans ses mémoires et s'en glorifie. Il n'a pas tort : c'est une des plus belles opérations de la ugerre. Mais il y a un détail qu'il ne dit pas, qui facilitait singulièrement sa tâche. Il connaissait le chiffre russe ; tous les ordres dans les armées de ses adversaires étaient transmis par T. S. F., il les déchiffrait et les connaissait en même temps que les exécutants. Tous les soirs, les radios interceptés étaient déchiffrés vers onze heures, on les portait à Ludendorff qui rédigeait alors ses ordres en conséquence. Lorsque par exception, il y avait quelque retard, il arrivait inquiet au Bureau du chiffre pour en connaître la cause. »

Il est facile de comprendre que la connaissance des ordres de l'ennemi facilite singulièrement la tâche du chef. Or, sans même avoir recours à l'espionnage, et à l'achat du dictionnaire employé par une puissance ennemie, la haute direction militaire peut, grâce aux spécialistes cryptologues qui travaillent pour elle, posséder les moyens de traduire les documents chiffrés avec les dictionnaires. En comparant soigneusement des centaines de documents, connaissant d'après l'heure de leur émission les objets possibles auxquels ils se rapportent, en faisant état de ce que dans une langue certains mots ou certains signes de ponctuation reviennent plus souvent que d'autres, les cryptologues arrivent à reconstituer les distionnaires, et les résultats obtenus pendant la guerre, par exemple la traduction de documents diplomatiques allemands dont a parlé la presse américaine, sont d'un ordre tout à fait ahurissant pour la majorité du public. Dans ces travaux, comme je l'ai dit, on fait des hypothèses sur le contenu des télégrammes et la signification de certains groupes. Donc tout ce qui peut orienter le décrypteur sur ces hypthèses est un bienfait pour l'ennemi, et une trahison de la part de celui qui a, par négligence, fourni cette orientation.

C'est ainsi que pour éviter de permettre de voir la tournure d'une phrase, la place des verbes ou des substantifs, il est rigoureusement interdit de mettre des mots en clair au milieu des groupes

chiffrés. Si vous télégraphiez : ce soir nous tenterons un 346 sur la première ligne ennemie, on devinera que 346 veut dire coup de main. Si, après une nuit tranquille, vous télégraphiez : nuit 251, rien à 339, on traduira : nuit calme, rien à signaler. Or ces erreurs-là, on les a faites couramment pendant la guerre, et souvent aussi lourdes et visibles que celles que je viens de signaler. La simple présence de conjonctions et de prépositions sert d'ailleurs puissamment les cryptologues, et doit être évitée dans les transmissions dont la captation est facile, comme celles des radiomessages.

On a fait mieux, et on l'a fait encore récemment à des manœuvres. Les correspondances radiotélégraphiques sont parfois transmises dans de mauvaises conditions : le poste récepteur peut être gêné par le bruit qui se fait dans le voisinage. Les groupes de chiffres sont erronés et ceux que l'on donne au déchiffreur, n'étant pas exactement ceux que le chiffreur a écrits, ne lui donnent la traduction que des phrases dénuées de sens. Dans ce cas-là, nous avons vu le destinataire demander qu'on lui envoie, *en clair*, le sens d'un groupe ou même tout le texte, et nous avons vu donner satisfaction à cette demande. Or, si l'ennemi n'était pas gêné dans sa réception il avait recueilli les groupes exacts, et n'avait qu'à rapprocher le clair du chiffré pour reconstituer le sens de ces groupes.

Une imprudence de ce genre doit être signalée aussitôt qu'on s'en aperçoit, pour permettre de changer les codes. Mais ce changement sera inutile, si les postes du front tombent dans une erreur que je vais vous signaler, et que nous n'avons pu extirper pendant la guerre.

Les postes de T. S. F., quand ils ont une communication à se passer, s'appellent par ce qu'on nomme un indicatif, un numéro.

Supposons que H. 28 soit l'indicatif du poste de l'infanterie divisionnaire de la 35e division, que D. 35 soit celui de l'Etat-Major de la 35e division. Le 1er poste appellera le 2e en émettant un certain nombre de fois D 35, D. 35... etc.. et commencera son message en annonçant son propre indicatif pour que D. 35 sache qui lui parle. Si l'ennemi sait que D. 35 est le poste de la 35e division, tant qu'il entendra appeler D. 35, il saura qu'il n'y a pas de relève et que D. 35, déjà fatiguée, est encore là.

Pour éviter cet inconvénient on a fait changer chaque jour les indicatifs. Le 1er du mois, nous avons pour nos indicatifs de nos 2 postes H. 28 et D. 35 ; le 2, K 19 et Z. 21 ; le 3, F. 12 et Q. 55, etc. suivant une liste que l'ennemi ne doit pas avoir. Le remplacement d'une division par une autre ne sera pas révélé par le changement d'indicatifs. Mais les imprudences interviennent. Tous les jours par exemple, de 8 h. à 8 h. 15 l'I. D. recueille les renseignements des régiments et, à 8 h. 20 exactement, appelle la division pour lui transmettre ces renseignements. L'ennemi, au bout de quelques jours, saura que le poste qu'on appelle à 8 h. 20, qu'il soit D. 35,

Z. 21 ou Q. 55, est le poste de la division, et durant toute la journée, les messages émis par ce poste-là seront les messages émis par la division, et on fera des hypothèses en conséquence. Pour le code, même genre d'imprudence. Tous les matins, un certain nombre d'éléments passent le même message chiffré ; nuit calme, rien à signaler. Faisons une hypothèse qui n'a rien de hasardeux. L'ennemi a trouvé dans un coup de main le code d'une unité du front abandonné dans un abri. De notre côté, prévenus de cette perte, nous avons mis en service un nouveau code où les lignes correspondant aux mots ne sont plus numérotées avec les mêmes groupes de chiffres. Les unités envoient donc des séries de groupes nouveaux pour dire : nuit calme, rien à signaler. Mais l'ennemi, avec l'ancien code, traduit les messages qu'il a captés les jours précédents et dont il n'avait pas la traduction ; il s'aperçoit qu'une unité donnée passe un message de cinq groupes tous les matins vers la même heure et que ce message est : nuit calme, rien à signaler. Il suppose que cette habitude n'a pas changé parce qu'on a changé le code et rapproche des nouveaux groupes le texte habituel, après une nuit qu'il sait aussi bien que nous avoir été calme : Il connaît ainsi cinq mots du dictionnaire et aura le moyen de faire des hypothèses sur toutes les phrases où un de ces cinq mots apparaîtra.

Il faut donc éviter avec le plus grand soin l'emploi de phrases que l'on appelle stéréotypées, c'est-à-dire l'emploi de formules toujours les mêmes constituant à travers tous les changements de dictionnaires un fil conducteur pour les cryptologues ennemis. Il y a lieu de remarquer du reste que ces formules peuvent s'appliquer à des sujets qui ne présentent aucun caractère d'urgence, que rien de mal n'arriverait si ces messages étaient transmis par une liaison régulière avec une ou deux heures de retard, et que c'est fréquemment un manque de prévoyance ou de sang-froid qui donne lieu à la transmission par télégraphe des communications ayant trait soit à des ravitaillements, soit à des renseignements : " néant " qui font souvent l'objet de formules stéréotypées.

L'abus des communications stéréotypées se rattache d'ailleurs à une autre erreur grave, c'est l'abus des communications tout court. Beaucoup d'unités possèdant un poste de T. S. F. n'ont jamais résisté au désir de le faire parler, même pour des sujets insignifiants. Bien que les progrès de la T. S. F. soient tels que les postes risquent beaucoup moins qu'autrefois de gêner leurs voisins, de brouiller les communications, il est toutefois des cas où les brouillages sont à craindre, quand ce ne serait que le brouillage de l'écoute des communications ennemies desquelles nous pouvons tirer parfois d'utiles informations. Mais il y a un autre danger au moins aussi grave : vous savez que la connaissance de la répartition des troupes ennemies sur le terrain, du front occupé par les divisions, des relèves, etc. est un des facteurs importants de la conduite des opéra-

tions. Plus il y a de postes T. S. F. dans un secteur, plus en général, il y a d'unités ; la présence de beaucoup de postes est donc un renseignement pour l'ennemi. Celui-ci, d'autre part, arrive lorsqu'un poste est bavard, à le bien connaître par le son de son émission, par des différences de manipulation d'un poste à l'autre, et même à situer sa position sur le terrain au moyen d'appareils spéciaux. Si le poste parle peu, son repèrage et son identification sont difficiles. S'il parle beaucoup, on le repère, on le bombarde et, en cas de relève, on s'aperçoit que le poste est changé, ce qui donne à supposer la relève. Un poste qui parle beaucoup est donc une source de renseignements précieux pour l'ennemi. Que dire des postes qui prennent la parole pour rien, pour des « appels », des vérifications d'appareils, pour échanger des phrases insignifiantes, et cela a été constant pendant la guerre. Ils se font repérer et leur situation est reportée sur une carte chez l'ennemi. Supposons maintenant que parmi nos procédés de chiffrement nous en fixions un pour les échanges de division à infanterie divisionnaire, un autre différent pour les communications d'infanterie divisionnaire aux règiments, et que nous trouvions moyen que ces deux procédés donnent des cryptogrammes d'aspect identique. Le cryptologue ennemi finit par s'apercevoir qu'il travaille sur deux systèmes et peut classer les documents de manière à n'utiliser que les communications entre deux postes donnés, toujours les mêmes, espérant ainsi arriver à élucider un système unique. Je vous ai dit qu'on changeait les indicatifs de nos postes ; il ne peut donc pas se fier aux indicatifs. Mais sur la carte il voit qu'une station existe à Carency, une autre à Lorette. Si ces stations sont bavardes on les repèrera tous les jours malgré que leurs indicatifs changent, et en travaillant sur Carency et Lorette seulement, que ce soit H. 22 ou W. 38 ou L. 17 ou P. 29, le décrypteur travaillera sur un seul code. C'est donc un crime non seulement à l'égard du personnel du poste si celui-ci est à portée du bombardement, mais à l'égard de toute l'armée, que de faciliter le repérage d'un poste d'émission. Quand un poste n'a rien à dire il doit se taire. De même que l'artillerie se tait pour ne pas se révéler et fait des réglages avec une seule pièce en la faisant tirer par surprise, de même les appareils de T. S. F. doivent-ils se montrer modestes et méfiants.

La multiplicité des messages chiffrés a, au point de vue technique, encore un autre inconvénient, celui de fournir des éléments de travail au décryptement ennemi.

Je vous ai dit que la science du décrypteur était basée sur l'examen et la comparaison des cryptogrammes, sur des statistiques des groupes figurant dans ces cryptogrammes. Plus il y a de documents, plus il y a de groupes, plus il y a d'éléments de statistique. Par exemple pour certains systèmes de chiffrement, il faut avoir deux cryptogrammes ayant exactement le même nombre de lettres

pour pouvoir trouver la clef ; plus on fera passer de télégrammes, plus l'ennemi aura de chances d'en trouver deux de même longueur, quel que soit le soin qu'apporte un poste donné à différencier les longueurs de ses communications, car un autre, peut-être sur un sujet tout à fait insignifiant, risque de passer un télégramme qui permettra par sa dimension au décrypteur ennemi centralisateur de toutes les interceptions de nos communications de trouver la clef qu'il cherche.

Il faut donc réduire les communications qui peuvent être interceptées à celles qui sont rigoureusement nécessaires. Bien entendu quand il y a nécessité de transmettre il ne faut pas hésiter, mais il faut être sûr de l'utilité. Il y a là un problème du même ordre que le suivant :

Afin d'éviter de multiplier les textes chiffrés, et pour tenir compte également des circonstances de combat par exemple où les combattants ont autre chose à faire que de chiffrer sous le feu pendant la progression et où l'arrière a hâte d'avoir des nouvelles, les instructions ministérielles laissent au commandement le soin d'autoriser dans certains cas l'emploi des messages en clair par T. S. F. ou T. P. S. Naturellement les messages passant en clair ne doivent pas renseigner l'ennemi, et dans la dernière guerre, l'envoi du message : « le crapouillot n° n'a plus de munitions » eut pour conséquence une attaque sur le point protégé par ledit crapouillot. Mais il y a lieu de bien se rendre compte de la valeur d'un message au point de vue du renseignement utile à l'ennemi. « Objectif atteint » par exemple, bien que l'ennemi sache que vous l'ayez repoussé, peut lui annoncer un moment de répit pour remettre votre troupe en ordre et lui donner l'idée de l'utiliser pour une contre-attaque.

L'emploi même de mots en clair dans une langue donnée, Français dans un secteur anglais par exemple, peut indiquer la proximité d'une relève et doit être complètement à éviter dans certaines circonstances.

On dit parfois au sujet des communications pendant le combat que l'ennemi a bien autre chose à faire que d'écouter ce que nous disons. C'est un manque d'appréciation complet : le spécialiste chargé de l'écoute considère que sa seule mission militaire, c'est l'écoute, et il ne la néglige pas plus au cours du combat que l'artilleur ne néglige son canon sous prétexte que les fantassins se battent ; et il n'y a pas que l'écouteur de T.S.F. déjà loin des lignes qui ait une conscience professionnelle, l'écouteur des téléphones en a une aussi et nous touchons ici à un autre des dangers qui menacent le chiffre.

Vous savez que la terre est un conducteur de courants électriques de valeur souvent fort élevée. L'emploi de la T. P. S. le prouve. Or, au début de la guerre les téléphones de campagne n'étaient montés qu'à une ligne. le courant de retour passait par la

terre et pouvait être capté par les écouteurs ennemis. On a pris de plus en plus de précautions contre des écoutes au cours de la guerre : on a imposé deux lignes dont une de retour au voisinage de l'ennemi, on a écarté les fils des parois des tranchées, etc. Mais les difficultés d'exécution, la fatigue du personnel, la boue, ont souvent empêché les troupes de respecter les consignes dont elles ne voyaient pas l'utilité. Ou bien l'exécution en était pire qu'une abstention ; c'est ainsi que des téléphones ont eu leurs fils de retour en contact avec des rails de lignes de chemin de fer, qui ne furent coupées que très tardivement ; mais, ce qui risquait de donner des renseignements à des postes d'écoute ennemis placés sur ces lignes. Quoiqu'il en soit des communications téléphoniques peuvent être surprises par l'ennemi. Pour masquer ces conversations on a eu recours au chiffre, mais on a permis de mélanger dans des messages téléphoniques le clair avec le chiffre, car des nombres prononcés sont beaucoup moins exposés à une écoute exacte que les transmissions par T. S. F. Il est alors utile bien entendu de ne pas répéter par trop un même groupe ce qui permet à un écouteur ennemi de bien le saisir, et de ne pas finalement donner le sens en clair : or, cela s'est fait constamment, soit comme confirmation, soit au cours d'une conversation faisant suite au message et où naturellement, les interlocuteurs ne se donnaient pas la peine de chercher des groupes dans une liste.

C'est pour répondre à des nécessités de ce genre qu'on a répandu l'emploi de mots de convention en désignant par des mots quelconques ou des noms de baptême les unités du front et certains points remarquables. C'est là un procédé à étendre à condition de changer assez souvent la nomenclature et qui devrait être employé aussi pour les formules stéréotypées dont je vous ai précédemment entretenu.

Cette question des noms propres est une de celles qui, dans les questions de chiffrement a donné lieu à de grosses difficultés pendant la guerre ; on ne peut naturellement faire figurer dans les listes de mots imprimés au service central tous les noms propres du front : On a alors recours pour les chiffrer au procédé suivant : On profite de ce que la liste contient des groupes pour représenter les lettres de l'alphabet, et on chiffre successivement toutes les lettres du nom. Ce procédé est long, et il a un grave défaut au vue cryptographique. Si l'on chiffre par exemple fort souvent un nom de localité violemment disputée, et contenant plusieurs fois la même lettre comme Nogent l'Abbesse, on reconnaît des séries de groupes qui se répètent dans beaucoup de télégrammes par exemple : 139. 435. 362. 111. 139. 624. 233. 051. 344. 344. 111. 662.662. 111 (Nogent l'Abbesse, les 2 b, les 2 s, les 3 e 111, etc..) avec des aspects caractéristiques, et on en déduit l'identification de certains groupes. On a donc laissé dans les listes un certain nombre de

lignes disponibles avec des numéros pour que dans chaque secteur on y inscrire les noms qui paraissent le plus souvent. Il faut se servir de préférence de ces numéros ou prendre des mots de convention qui n'aient pas l'aspect caractéristique des noms figurant sur la carte lorsqu'on les chiffre (car il faut les chiffrer pour la T. S. F.) de manière à ne pas laisser faire d'hypothèses sur les groupes qui les précèdent et les suivent et qui le plus souvent sont les prépositions a ou de par exemple. Quand on dispose de plusieurs groupes pour chiffrer une même lettre ou qu'on a le chiffrement de syllabes entières, il faut varier le chiffrement d'une fois à l'autre. Enfin lorsqu'on a chiffré une première fois un nom et qu'il n'y a pas d'ambiguité possible, il faut ne plus chiffrer que la première lettre quand le mot se répète. En un mot il faut faire tout ce qu'on peut pour éviter la répétition de séries de groupes caractéristiques dans un cryptogramme.

Si les conseils donnés pour le chiffrement étaient toujours suivis, si l'on n'abusait pas des communications chiffrées, si on évitait les répétitions, si on ne donnait pas par des coups de téléphone imprudents d'indications sur la contexture du chiffre, un code constitué comme nous l'avons dit pourrait durer quelques semaines, dans les circonstances de la guerre de positions, à condition bien entendu que l'ennemi ne s'en procure pas un exemplaire. Mais, à cause des imprudences, les décrypteurs arrivent assez vite à fournir des renseignements. Comme on ne peut pas passer son temps à changer les dictionnaires, on a cherché un moyen d'en augmenter la durée et c'est pour cela qu'on a imposé le surchiffrement.

Le surchiffrement, ou double chiffrement, est une opération qui consiste, lorsqu'on a établi un cryptogramme au moyen par exemple d'un code, en remplaçant les mots du clair par les groupes qui les représentent, à soumettre ce cryptogramme à une nouvelle opération qui en modifie les caractères (par exemple remplacement de chiffres par des lettres) ou qui trouble l'ordre de ceux-ci. Le but de cette opération est de diminuer ou même de faire disparaître les répétitions de groupes identiques.

Le système de surchiffrement qui était règlementaire à la fin de la guerre, pour les codes mis entre les mains des unités, était le suivant : Un tableau répartissait entre les 10 chiffres de 0 à 9, qui formaient les groupes du code, les 26 lettres de l'alphabet, si bien qu'à chaque chiffre correspondaient 2 ou 3 lettres. On remplaçait les chiffres par une de ces lettres au hasard, et ainsi un groupe de 3 chiffres pouvait être représenté par plusieurs groupes de 3 lettres différents (jusqu'à 27)

Par exemple si 1 correspond à C N U

Par exemple si 7 correspond à D P Z

Le groupe 177 peut être représenté par C D P ou U D P, ou N P Z. Ainsi on masque les répétitions d'un même groupe et même la répétition d'un même chiffre dans un groupe. Au déchiffrement, on fait l'opération inverse, et comme à chaque lettre ne correspond qu'un seul chiffre, on retrouve les groupes correspondans, dans le dictionnaire, au texte clair primitif.

C'est là une méthode de surchiffrement, il peut y en avoir bien d'autres. On peut suivant la place d'une chiffre dans le groupe, par exemple, suivant qu'il est le 1er, le 2^{e} ou le 3^{e}, employer une série différente de lettres pour le représenter, on peut mélanger suivant une loi connue les chiffres de chaque groupe, etc. Mais, quel que soit le système de surchiffrement employé, il importe d'éviter là encore les imprudences qui peuvent le déceler.

Avant d'insister sur ces imprudences, j'appellerai votre attention sur l'utilité d'employer le double chiffrement. En principe, ce procédé était obligatoire pendant la guerre pour les radios. le chiffrement simple, par suite des répéditions trop nombreuses dûes aux maladresses signalées plus haut, risquant de permettre à l'ennemi de reconstituer trop vite une grande partie du texte de nos télégrammes. Dans la pratique, on a relativement peu surchiffré, parce que les exécutants n'admettaient pas l'utilité de ce travail supplémentaire. Or, il faut se convaincre du fait suivant : c'est qu'on est libre, en foulant toutefois aux pieds les règles de la discipline, de donner à l'ennemi en transmettant en clair des renseignements qu'il peut utiliser pour vous tirer dessus, mais il n'est pas loyal, par paresse, de chiffrer assez mal pour lui fournir des éléments suffisants pour lui permettre de traduire les télégrammes des camarades du front qui, se servant bien du chiffre, ont confiance dans la sécurité de leur dictionnaire. Le mépris du double chiffrement n'est donc pas, comme le disent les Anglais, le fait d'un gentleman.

La négligence dans le double chiffrement a, au cours de la guerre, entraîné des conséquences étranges, et c'est là le danger auquel j'ai fait allusion tout à l'heure. Il est arrivé que, au cours de transmissions successives, un télégramme parti en chiffrement simple ait été surchiffré par une autorité soucieuse des règlements et que cette opération faite sans soin ait été funeste au secret du surchiffrement. Je m'explique : il est arrivé ceci dans un secteur du front. Une unité du front téléphone en clair un renseignement à son régiment. Nos postes d'écoute ont intercepté la communication dans des conditions telles que l'ennemi a pu également la surprendre. Le P. C. du régiment a chiffré le renseignement, mais en chiffrement simple, et la présence d'un nom de pays caractéristique, figurant 2 fois et chiffré 2 fois de la même manière permettait d'identifier le clair recueilli par téléphone avec le chiffre transmis par T. S. F. à l'infanterie divisionnaire. Celle-ci a repris le

renseignement pour l'envoyer à la division, mais l'a surchiffré correctement pour une transmission T. S. F. Seulement elle en a annoncé l'origine en mettent en tête en clair : de H 26 à Z 35 à telle heure H. 26 et Z 35 étant les indicatifs du P. C. et de l'infanterie divisionnaire, si bien que cette série de transmissions d'un clair, d'un mal chiffré, d'un bien chiffré avec indications d'origine et d'heure livrait tous nos systèmes de chiffrement sur ce point du front.

Il faut donc éviter tout ce qui peut permettre d'identifier un télégramme surchiffré, ou chiffré avec un procédé spécial, avec une communication en clair ou non surchiffrée. A cet effet, il faut non seulement chiffrer les indications d'origine primitive si l'on veut les transmettre, mais changer le texte clair à rechiffrer en en modifiant la longueur et la tournure si possible, de manière à avoir un cryptogramme plus long ou plus court que le précédent, et à n'y pas présenter les mots dans le même ordre.

Si une première expédition d'un télégramme n'est pas parvenue à destination et qu'on en envoie une autre quelques heures plus tard, il faut avoir soin de renvoyer rigoureusement le même chiffrement avec les mêmes groupes ou les mêmes lettres, ou de changer complètement le texte comme longueur ainsi que le numéro si l'on en met un en tête. Si en effet on surchiffre les groupes en prenant la première fois une lettre pour représenter un chiffre, puis la seconde fois une autre des lettres qui correspondent à ce chiffre, on peut fournir à l'ennemi des éléments pour retrouver le surchiffrement, Si 3 correspond à M, V ou Z et qu'on surchiffre dans le 1er télégramme le groupe 237 par A MP, dans le 2e par A V P, la comparaison donnera à penser que M et V correspondent au même chiffre, et par ce moyen on retombera rapidement sur 10 groupes de lettres équivalentes, et sur la reconstitution du tableau de surchiffrement.

Tant pour la sécurité du chiffrement que pour celle du surchiffrement, il faut éviter de fournir à l'ennemi les comparaisons entre les clairs et les cryptogrammes. Nous avons vu que le téléphone est un danger à ce sujet. Mais il en est d'autres. Il faut avoir soin de ne pas laisser traîner dans les P. C. ni dans les poches de papiers portant le texte d'un cryptogramme et sa traduction par exemple. Tout ce qui est inutile pour les opérations, feuilles ayant servi au chiffrement ou au déchiffrement, cryptogramme dont la traduction a été faite et sur lequel l'accord est complet avec le correspondant, renseignements périmés ou sans importance, tout cela doit être soigneusement et rapidement détruit et détruit de manière sûre. A la guerre il faut toujours se méfier de vieux papiers.

Les renseignements et les avis que je vous ai donnés jusqu'ici portent sur les mesures de sécurité relatives à nos chiffres: Si l'on vous invite à prendre de telles précautions, c'est qu'on a eu

l'occasion d'étudier les moyens de saisir chez l'ennemi d'utiles renseignements par la voie de sa correspondance cryptographique. Il est donc important, lorsque lui-même est en défaut sur ce point, de fournir à nos services de décryptement les éléments qui peuvent permettre à ceux-ci de mener à bien leur tâche délicate. Or, vous pouvez avoir sur ce point une action efficace.

Il n'est pas du ressort des armes engagées dans l'action immédiate de chercher à capter les communications T. S. F. ennemies. Une organisation spéciale est créée dans ce but. Mais la proximité de l'ennemi peut mettre l'infanterie et l'artillerie à même de connaître bien des renseignements qui intéressent le service de décryptement : conversations surprises par des patrouilles, tentatives de coups de main, observations à la suite de réglages d'artillerie suivis par une antenne et pouvant se rapporter à des incidents du règlage, etc. Surtout l'infanterie est la première à entrer dans les P. C. ennemis. Or, il a été lamentable pour un cryptologue de voir comment les papiers des P. C. ont été dispersés sans utilité pour personne par les gens qui y ont pénétré. Cela a été le gaspillage des renseignements les plus précieux : si l'on ne voulait pas, comme cela aurait dû être fait, rassembler les papiers et les envoyer au 2e Bureau de la division, du moins était-il inutile de les précipiter dans la boue et dans les feuillées voisines. Les carnets trouvés sur les morts et gardés comme trophées (tristes trophées trouvés dans les poches, et par ceux qui avaient le temps et le loisir d'y fouiller) contenaient souvent des renseignements précieux qui sont tombés par hasard après la guerre dans les mains d'un idoine du chiffre, alors qu'ils ne pouvaient plus servir à rien. L'action des officiers peut être des plus précieuses pour cet objet, la réunion et la transmission des renseignements. Je ne veux parler que pour mon service, mais il est bien certain que la question n'intéresse pas que ce dernier, et le raisonnement si fréquent : « Il y a tant de sources de renseignements qu'un carnet de plus ou de moins n'a aucun intérêt » est absolument faux. Le carnet d'un des officiers du chiffre de l'ennemi, si celui ci a l'imprudence d'y noter les clefs des systèmes de cryptographie, ne sera remplacé par aucun autre document dans tout un corps d'armée. Pour me résumer donc sur ce point, il est d'une importance capitale de ne pas avoir ce sentiment bizarre mélangé de laisser-aller et d'une sorte de pudeur de se mettre en avant, qui consiste à négliger tout ce qui paraît de nature à fournir des renseignements sur les chiffres ennemis.

Abandonnant ce sujet, et approchant de la fin de la conférence, je vous signalerai encore, afin de bien vous pénétrer de cette idée, la nécessité de traiter le chiffre, qui est un service secret, avec les précautions qu'exige le secret. Il ne faut pas parler inconsidérément devant des tiers du contenu des cryptogrammes traduits. Au début de la dernière guerre, nous avons réussi à donner à

l'Etat-major la traduction des ordres du G. Q. G. allemand. La presse, renseignée par des bavardages, a parlé de renseignements obtenus par la tratuction de radiotélégrammes allemands, et cette source si précieuse de documentation a été tarie.

Il ne faut pas laisser voir aux hommes les codes ou les modes de chiffrement ni en parler devant eux. Ils peuvent être faits prisonniers et parler de ce qu'ils savent, Or, il est intéressant pour l'ennemi de savoir si nous avons toujours le même système à codes et si nous changeons souvent ceux-ci, ce que des surchiffrements régulièrement faits peuvent lui cacher. Le remplacement des codes fut parfois un indice d'attaque prochaine. Il ne faut pas laisser perdre des carnets. On en a perdu beaucoup et, bien que les comptes rendus aient signalé par exemple que l'exemplaire n° tant avait été enterré par un obus, et par suite détruit, on a parfois retrouvé l'exemplaire n° tant dans un hôpital, apporté par un blessé, et même en 1918 dans un hopital allemand : manque de franchise qui a pû permettre à l'ennemi de lire nos télégrammes, puisque l'exemplaire étant supposé détruit, on n'avait pas mis un autre code en service. Il faut admettre qu'il a toujours existé des espions parmi les troupes et que ceux qui ont été pris étaient jusqu'aux premiers soupçons considérés comme du personnel de toute sécurité par leurs chefs et leur entourage : il ne faut donc pas s'endormir béatement dans la confiance et un des devoirs du chef est de garder pour lui les secrets dont il est responsable. Une vigilance active sur les documents du chiffre est nécessaire, et l'on doit signaler en toute confiance et en toute rapidité tous les incidents qui donneraient à douter du secret, comme une communication téléphonique imprudente sur le contenu d'un télégramme. L'autorité supérieure jugera des mesures à prendre.

En terminant cette conférence, où il n'a été question je vous le rappelle que des procédés de chiffrement prévus pour les unités du front, le chiffre des grands états-majors étant soumis à des règles spéciales, je résume les précautions dont j'ai tenté de vous montrer l'utilité. Ne pas abuser inutilement de la correspondance chiffrée qui peut fournir des éléments de travail aux décrypteurs ennemis, chiffrer correctement comme il est dit dans les instructions relatives au système cryptographique règlementaire à un moment donné, éviter tout ce qui peut révéler à l'ennemi le contenu d'un cryptogramme, soit immédiatement par des conversations ou des demandes d'explication imprudentes, soit ultérieurement par l'abandon de papiers compromettants. Les consignes données sur ces sujets sont souvent ennuyeuses et même difficiles à respecter : elles ne sont données par l'administration centrale que lorsque l'expérience en a démontré la nécessité. Sur ces points il ne suffit pas dire, comme on le fait parfois « Il est évident que de telles précautions sont exagérées. » Elles ne sont imposées que lorsque, faute qu'elles aient

été prises, des correspondances ont été l'objet d'indiscrétions. On connaît d'ailleurs à la Section du Chiffre les inconvénients que certaines d'entre elles présentent pour les corps de troupes, et des études y sont constamment en cours pour chercher à concilier les deux objets contradictoires : mettre aux mains de nombreux exécutants peu familiarisés avec la cryptographie des méthodes de chiffrement simples, et assurer la sécurité du secret malgré les imprudences et les maladresses.

Afin de guider les officiers des corps de troupe dans l'emploi du chiffre, et afin d'assurer le service du chiffre dans les Etats-Majors, on a décidé d'adjoindre à chacun de ceux-ci un officier de complément, ayant reçu une instruction spéciale et particulièrement chargé des questions techniques de chiffrement. Le recrutement de ces officiers est en cours. L'Etat-Major de l'armée a organisé une école d'instruction du chiffre analogue à celle-ci, mais où les éléments sont répartis en séries successives d'un effectif limité. Le recrutement s'étend aux lieutenants et capitaines, en principe âgés de plus de 28 ans : les officiers, après avoir suivi le cours et avoir montré qu'ils peuvent être employés avec fruit dans le service, pourront être classés dans le service d'Etat-Major et feront leurs périodes, s'il y a lieu, au titre du chiffre. Au cas où ces conditions paraîtraient intéressantes à quelques uns d'entre vous, je les prierai d'écrire au chef de la Section du chiffre de l'E. M. A., Ministère de la guerre, qui entrerait en relation directe avec eux pour leur donner quelques détails sur l'organisation des cours et, au besoin, sur les demandes à faire pour passer au service du chiffre.