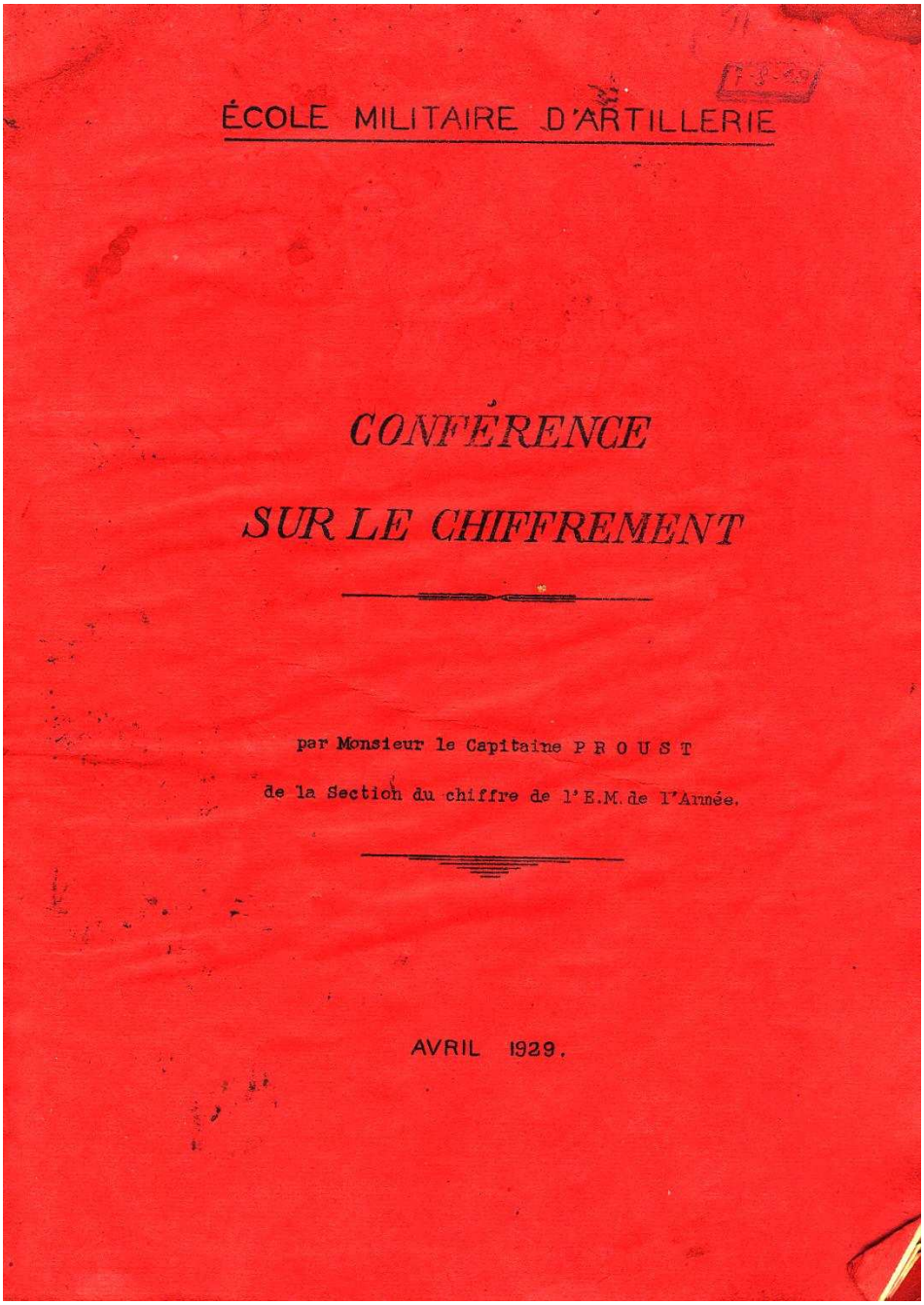
La conférence du capitaine Proust devant l'école militaire d'artillerie en avril 1929.

Par Daniel TANT



ÉCOLE MILITAIRE D'ARTILLERIE

CONFÉRENCE

SUR LE CHIFFREMENT

par Monsieur le Capitaine P R O U S T

de la Section du chiffre de l'E.M. de l'Armée.

AVRIL 1929.

I - NÉCESSITÉ DE CHIFFRER

1°.- Les conditions de la guerre moderne concourent à rendre de plus en plus difficile l'exécution de la liaison entre les différents échelons du commandement et les différentes armes :

Puissance du feu,

Etendue du champ de bataille,

Emploi de masques artificiels et de gaz,

Longue portée des matériels nouveaux,

Action de l'aviation

etc .....

Cette liaison entre les P.C., les observatoires et les troupes étant absolument indispensable à l'exercice du commandement, il a fallu multiplier les moyens de transmission en faisant état de tous les progrès scientifiques réalisés en cette matière.

2°.- Caractéristiques des moyens de transmission.-

Télégraphie avec fil : Assure bien le secret.

Téléphone : Permet le secret des communications quand il est installé avec fil de retour. A un seul fil, il est indiscret.

Optique : Assure bien le secret dans la liaison avant-arrière, mais les communications arrière-avant sont lues par l'ennemi.

Chiens et pigeons : Liaison très précaire, les animaux porteurs de messages pouvant s'égarer dans les lignes ennemies.

T.S.F. et T.P.S. : Procédés radio-électriques qui possèdent le grave défaut d'être très indiscrets, l'ennemi les entendant aussi bien que nous.

3° - L'ennemi dispose pour ses écoutes :

de postes spéciaux pour capter les transmissions téléphoniques et de T.P.S.;

de postes spéciaux pour capter les transmissions par T.S.F. avec installations radio-goniométriques;

de personnel spécialisé dans l'étude des télégrammes captés.

4° - Il est donc nécessaire, si l'on ne veut pas que l'ennemi profite de nos renseignements et de nos ordres, que le langage tenu par nos organes d'émission ne lui soit point compréhensible, d'où obligation de chiffrer les télégrammes susceptibles d'être captés.

5° - La Guerre de 1914-1918 fourmille d'exemples d'imprudences commises dans cet ordre d'idées.

Par exemple :

a)- Le Général VON MARWITZ Commandant la cavalerie de l'aile droite allemande en Août 1914 passe quantités de radios en clair. D'autres armées font de même. Captés par nous, ces radios donnent au Commandement français des renseignements importants;

b)- Pendant l'hiver 1915-16, le Service des écoutes de la 10° Armée française qui avait installé un poste d'écoute dans le village de NEUVILLE SAINT WAST, recueille quantité d'ordres préparatoires allemands téléphonés et apprend même l'heure H de l'attaque.

Conséquence : Contre-préparation de notre artillerie et à l'heure H, arrosage intensif de la tranchée de départ. L'attaque ne sortit pas;

c)- Le 12 Juin 1918, un poste français passe le radio suivant, sommairement chiffré, et contenant des mots en clair :

" Demande de ravitaillement pour le 14, gare de VERBERIE. 3 rames à répartir entre les éléments du 18° Corps; 80 caisses, 22 sacs pour ARBANERE, 100 caisses et 40 sacs pour de SALINS ".

Les allemands identifient ainsi le 15° C.A. et 2 des D.I. qui le composent (15° D.I.,Général ARBANERE et 38° D.I., Général de SALINS).

II - CONSIDÉRATIONS GÉNÉRALES SUR LE CHIFFRE

1° - Son but est d'assurer :

a)- le secret de nos communications par des procédés sûrs :

C'est le Chiffre proprement dit;

b)- les recherches sur les procédés de chiffrement de l'ennemi et, si possible, la traduction en clair de ses télégrammes chiffrés :

C'est le Décryptement.

2° - Il importe tout d'abord de préciser le sens de certains termes employés en matière de chiffre, faute de quoi on se comprend mal.

Chiffrement : Opération par laquelle on transforme un texte rédigé en langage clair en un texte incompréhensible à quiconque n'est pas dans le secret du procédé. Ce dernier texte s'appelle texte chiffré ou cryptogramme.

Déchiffrement : Transformation du cryptogramme en langage clair. C'est l'opération inverse de la précédente.

Décryptement : Opération de déchiffrement faite par celui qui n'est pas au courant du procédé de chiffrement employé.

Cryptologue : Personne qui se livre à des opérations de décryptement.

Cryptographes : Appareils à chiffrer (réglettes, cadrans, machines à chiffrer).

3° - Ce n'est pas seulement de nos jours que l'on chiffre. Dans l'antiquité grecque on chiffrait. Jules CESAR a donné nom à un procédé de chiffrement; au Moyen-âge, le chiffre était fort en honneur à ROME et dans les petites cours italiennes.

On a aussi beaucoup chiffré pendant les guerres du 1er Empire, pendant la guerre de 1870-71 et pendant la guerre de 1914-18.

4° - Les procédés de chiffrement peuvent se ranger en deux grandes catégories :

a)- Système de transposition.- modification dans l'ordre des lettres du clair suivant une loi fixée par une clef connue des deux correspondants.

Exemple : Soit à chiffrer par transposition à tableau : "Ravitaillement de la troisième division gare NANCY" avec le mot-clef : "MARSEILLE".

Clef littérale : M A R S E I L L E

Clef numérique : 7 1 8 9 2 4 5 6 3

R A V I T A I L L

E M E N T D E L A

Texte clair : T R O I S I E M E

D I V I S I O N G

A R E N A N C Y

Cryptogramme obtenu par relèvement de haut en bas des colonnes du clair dans l'ordre des nombres de la clef numérique :

AMRIR TTSSA LAEGA DIINI EEOCL LMNYR NTDAV EOVEI NIIN;

b)- Systèmes de substitution : Respectant l'ordre du clair, on en remplace les caractères par des signes spéciaux.

Exemple : Soit à chiffrer en substitution simple :

" L'ennemi recule " avec la clef de substitution ci-dessous :

	1	5	3	2	4
4	a	b	c	d	e
5	f	g	h	i	j
2	k	l	m	n	o
1	p	q	r	s	t
3	u	v	x	y	z

on a le chiffrement suivant :

L	E	N	N	E	M	I	R	E	C	U	L	E
25	44	22	22	44	23	52	13	44	43	31	25	44

Ce système comporte une infinité de variantes, destinées à compliquer le procédé ou à réduire le temps consacré au chiffrement.

C'est ainsi que pour diminuer le temps consacré au chiffrement et réduire la longueur des télégrammes, on substitue mot par mot au lieu de lettre par lettre, en faisant usage d'un répertoire chiffré.

Exemple :

L	ennemi	recule
143	510	301

(chiffré avec un répertoire de 1000 mots représentés par des groupes de 3 chiffres).

III - PROCÉDÉS EN USAGE DANS LES PETITES UNITÉS.

1° - Les procédés en usage aux armées, et en particulier dans les petites unités, consistent dans l'emploi des répertoires.

On appelle dictionnaires les répertoires ayant un vocabulaire très riche pouvant aller jusqu'à 100.000 mots ou expressions.

codes ceux dont le vocabulaire ne dépasse pas 10.000 mots ou expressions.

Exemple : le code 67, distribué dans les petites unités jusqu'à l'échelon régiment d'Infanterie, bataillon formant corps, groupe d'artillerie, ballon, escadrille inclus.

carnets ceux dont le vocabulaire est inférieur à 1000 mots ou expressions.

Exemple : le carnet de chiffres M^le^ 1924 dit carnet 333 utilisé aux échelons inférieurs non dotés de codes.

2° - Les dictionnaires, codes et carnets sont de deux types:

a)- répertoires ordonnés

possédant une seule table pour le chiffrement et le déchiffrement.

Les mots du clair sont écrits dans leur ordre alphabétique :

a, ab, abandon, ... zone, zouave,

et leur représentation chiffrée est en regard dans l'ordre numérique :

a:000, ab:001, abandon:002 .... zone:998, zouave:999.

b)- répertoires désordonnés ou bâtons rompus

possédant deux tables :

table de chiffrement : les mots du clair sont dans l'ordre alphabétique, leur représentation chiffrée est dans un ordre quelconque :

a:426, ab:163 ..... demande:862 ..... mitrailleuse:001... zouave:234;

table de déchiffrement : les nombres de 3 chiffres sont dans leur ordre numérique et les mots du clair se trouvent par suite dans un ordre non alphabétique :

001: mitrailleuse ..... 163: ab ..... 234: zouave ..... 426: a ..... 862: demande;

c)- Syllabage.- Il est impossible de faire figurer dans un répertoire de 1000 ou même 10.000 groupes tous les mots du langage, en particulier les noms propres.

Comment chiffre-t-on un mot que l'on ne trouve pas dans le répertoire ?

En le syllabant, c'est-à-dire, en chiffrant successivement les différentes lettres et syllabes de ce mot.

Exemple : le mot "embarquement" ne figure pas dans le carnet 333, il sera chiffré ainsi avec ce carnet :

em	ba	r	que	ment
735	859	038	558	387

3° - Répétitions.- Les travaux des décrypteurs étant basés sur les répétitions, il faut les éviter.

a)- Syllabage.- Dans le chiffrement par les petites unités, le syllabage s'applique fréquemment à des noms propres (termes géographiques, notamment) qui pourront se trouver répétés dans plusieurs télégrammes. Ces répétitions aideront à la reconstitution des répertoires.

Exemple : Les écoutes d'une Division ennemie opérant dans la région de SOISSONS font ressortir la répétition dans de nombreux télégrammes passés par T.S.F. de la suite

196 023 624 196 517 196

On pourra faire l'hypothèse que cette suite, qui comporte la répétition du groupe 196 est le chiffrement de "SOISSONS"

On en déduira que 196 = S
023 = O
624 = IS
517 = ON

et ces hypothèses appliquées à d'autres parties de télégrammes où figurent ces groupes pourront aider à reconstituer d'autres mots.

On devra donc s'efforcer, lorsqu'il faudra syllaber, de "découper" le mot en tranches différentes pour éviter que l'ennemi fasse des rapprochements tels que celui indiqué ci-dessus.

SOISSONS pourra être syllabé S OI SS ON S
puis SO IS SO N S
puis S O IS SO NS

etc .....

Les répétitions disparaîtront dans le même télégramme. Mais il ne faut pas oublier que tout le monde dans la Division, et peut-être dans les Divisions voisines, parle de SOISSONS, aussi

malgré les précautions individuelles il y aura des répétitions certaines, le découpage de SOISSONS présentant un nombre de solutions limité;

b)- Formules stéréotypes.-

Les commencements et fins de télégrammes ne devront pas être uniformément rédigés de la même manière,et on évitera notamment l'emploi habituel des termes ci-après :

"J'ai l'honneur de ....

"Je vous prie de .....

"Suite à télégramme N° ....

"Pour telle autorité ....

"FIN".

"Signé : X.

"Rendre compte".

c)- Employer le style télégraphique.-

Dans les textes courts, il y a moins à craindre la fréquence de certains mots. Par exemple, ne pas chiffrer "Le Colonel Commandant le 152° Régiment d'Infanterie .....

mais chiffrer "Colonel 152° R.I. .....

d)- Formules grammaticales.-

N'employer qu'en cas de nécessité absolue pour la compréhension du texte les signes de ponctuation et les termes grammaticaux (singulier, pluriel etc..) dont la fréquence fait deviner le sens et qui "découpent" le télégramme.

4° - Surchiffrement.- Pour supprimer ou tout au moins atténuer les répétitions, on emploie le surchiffrement.

a)- Un télégramme étant chiffré en groupes de chiffres au moyen d'un répertoire, on remplace ces chiffres par des lettres

prises dans un tableau dit de surchiffrement.

Exemple de tableau de surchiffrement.

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

Le mot SOISSONS chiffré :

196 023 624 196 517 196

devient

XHN KAQ MAZ IHN JIG IDY

ou encore

IHY LSF YSR XDN BXC XHM

On voit que les répétitions 196 .... 196 .... ont disparu à la suite de leur remplacement par des groupes de lettres.

Le procédé de surchiffrement est celui du carnet de chiffre des petites unités.

Pour le code 67, le surchiffrement se fait en remplaçant chaque groupe de 2 chiffres par un groupe de 2 lettres pris dans un tableau de correspondance comprenant les nombres de 00 à 99.On peut d'ailleurs imaginer quantité d'autres procédés de surchiffrement plus ou moins compliqués.

b)- Le surchiffrement n'a pas que cet avantage, il permet de conserver un répertoire dont la sécurité est douteuse. Le simple changement du tableau de surchiffrement modifie entièrement la physionomie des groupes de lettres et prolonge pendant quelque temps la sécurité du répertoire;

c)- En Août 1914, les Russes utilisaient en Prusse Orientale un dictionnaire chiffré que les Allemands connaissaient. Les ordres russes passés par T.S.F. chiffrés avec ce code qui n'était

pas surchiffré étaient lus par les Allemands, déchiffrés immédiatement et communiqués au Général LUDENDORF qui donnait ses ordres en conséquence.

5° - Imprudences.-

a)- Ne jamais mélanger le clair et le chiffré;

b)- Si un télégramme mal chiffré doit être répété, le chiffreur ne doit pas se contenter de rectifier l'erreur et réexpédier le télégramme. L'étude comparée des 2 télégrammes par un décrypteur ennemi lui donnerait de précieux renseignements sur le procédé de chiffrement.

Dans un tel cas, il faut rédiger un nouveau télégramme en modifiant le texte clair (sans en changer le sens bien entendu) lui donner un autre numéro afin que l'ennemi ne se doute pas qu'il s'agit de la répétition du premier.

6° - Plan de chiffrement.-

L'emploi du carnet de chiffre avec surchiffrement dans les petites unités ne présente pas de difficultés, mais il demande du temps. Son utilisation est prévue pour la correspondance chiffrée en période de stationnement et en période calme.

En période de combat, où les conditions matérielles d'installation des P.C. sont presque toujours défectueuses, où il faut transmettre vite des ordres et des comptes-rendus, où les termes géographiques et les noms propres sont très nombreux, l'emploi du carnet de chiffre devient difficile.

C'est pour ces raisons que, dans ces périodes d'opérations actives, il n'est employé que tout à fait exceptionnellement.

On le remplace par le plan de chiffrement.

De même que le commandement pour une opération quelconque fait une série de plans (plans de feux, de ravitaillement en munitions, plan d'engagement de l'Infanterie,etc...) de même doit-il préparer, à tous les degrés, un dispositif pour assurer la sûreté et la rapidité des liaisons. Il doit prévoir les divers renseignements et les divers ordres afférents au développement de l'opération,en tant qu'ils entrent dans les prévisions humaines,et en faire une liste où chacun d'eux sera représenté par un groupe de lettres.

Exemple : Un détachement de découverte fera figurer sur son plan des expressions de la lecture de celle ci-dessous.

L'ennemi occupe les ponts de la Marne = KPAC

Il ne les occupe pas = KRIN

L'ennemi occupe les ponts de la Vesle = KBGH.

Autre exemple : Pour un coup de main d'Infanterie on fera un plan de chiffrement comportant les expressions ci-après :

Tranchée ennemie atteinte, elle est vide = LMBA

Je me porte sur la deuxième tranchée, allongez l'encagement = LPRF.

L'ennemi contre-attaque sur ma droite, faites-y tirer l'artillerie = LZIK

etc .....

Autre exemple encore :

L'Officier d'artillerie,de liaison près de l'unité d'Infanterie,demande au Chef de celle-ci : Quels feux d'artillerie vous seront nécessaires au cours de l'opération ?

L'autre répond : 1er objectif, cette ferme. 2e le verger à droite. Il faudra tirer sur ces deux régions et sur la lisière

du boqueteau à gauche. L'Officier de liaison avec 2 feuilles de papier et un carbone fait un croquis approximatif et y écrit aux points convenables : Objectif de tir N° 1, objectif de tir N° 2, objectif de tir N° 3. Il met en légende :

Commencez tir N° 1 = ABCY

Cessez tir N° 1 = ALZD

Commencez tir N° 2 = APQR

etc ....

Ces plans de chiffrement peuvent permettre de dire en un groupe beaucoup de choses, et des choses précises sur la manoeuvre prévue.

Ces plans rentreront par leurs signaux très brefs dans les conditions optima des communications radios. Ils pourront tout aussi bien être utilisés par des signaleurs à bras en des points où l'installation de postes de T.S.F. est impossible.

La condition à respecter est que 2 unités voisines ne donnent pas à un même signal des sens différents, aussi une répartition des groupes entre les unités doit-elle être faite par le commandement.

Le plan de chiffrement est établi par la Division qui le diffuse jusqu'à l'échelon bataillon et groupe d'artillerie.

Ces unités utilisent les groupes mis à leur disposition pour les compléter suivant leurs besoins propres.

Etabli pour opération déterminée, il sera utilisé pendant peu de temps car les conditions nouvelles du combat (qui se déroulera peut-être sur un autre terrain avec des unités différentes) ne permettront plus l'emploi du plan établi quelques jours avant.

A ce moment, la Division établira un nouveau plan correspondant à la nouvelle situation.

Le plan de chiffrement est employé en combinaison avec les expressions condensées chiffrées de l'Instruction provisoire sur les liaisons et transmissions dont il est question ci-après (paragraphe 6).

7° - Signalisation.-

L'instruction provisoire sur les liaisons et transmissions du 26 Mai 1923 contient dans ses annexes une certaine quantité de signaux conventionnels et les signaux Morse qui leur correspondent.

Elle contient aussi des messages conventionnels en groupes de 3 lettres = ART = artillerie, AVI = avion, etc ....

Ces signaux et messages conventionnels ne sont pas du chiffre. C'est du langage abrégé, n'donnant aucun secret aux communications.

Les messages conventionnels faits au début de la guerre pour les avions ne répondent pas toujours bien aux conditions de l'action à terre. Leur nombre est beaucoup trop limité pour permettre leur utilisation dans toutes les circonstances du combat.

Chiffrés par les soins de l'Armée et employés avec les expressions du plan de chiffrement, ces signaux et messages servent aux communications des petites unités au combat sans emploi du carnet de chiffre.

L'instruction du 26 Mai 1923 sur les liaisons et transmissions étant en cours de refonte, il n'y a pas lieu pour le moment d'insister davantage sur ce sujet.

IV - CONSIGNES TECHNIQUES DE SÉCURITÉ.

1° - Conserver les documents en lieu sûr et à l'abri des vues.

2° - Ne pas confier le travail de chiffrement à une personne non qualifiée.

3° - Détruire tous les brouillons de chiffrement après expédition du télégramme. Ne jamais écrire sur la même feuille de papier le clair et le chiffré du même télégramme.

4° - En cas de crainte de capture par l'ennemi, détruire les documents en les brûlant ou en les enterrant.

5° - Si on change les documents, ne pas oublier de rendre ceux qui sont périmés.

6° - Faire parvenir au commandement sans retard tous documents du Chiffre qui seraient trouvés au cours d'une avance dans les P.C. ennemis.

7° - En cas de perte ou de capture de documents par l'ennemi, en rendre compte sans délai.

V - PERSONNEL DU CHIFFRE AUX ARMÉES

1° - Les Etats-Majors des grandes unités disposent de personnel spécialisé

a)- Officiers de l'Armée active;

b)- Officiers de réserve instruits en temps de paix.

2° - Les petites unités ne disposent pas de personnel exclusivement consacré au fonctionnement du service du Chiffre.

Le service est assuré dans les E.M. d'A.D., de Régiment, d'I.D., de Groupe et de Bataillon par du personnel des postes de commandement instruit en temps de paix.

Il est constitué avec ce personnel un atelier de chiffrement à chaque P.C.

VI - CONCLUSION

Le but principal de cette conférence est de montrer la nécessité de chiffrer, et surtout de bien chiffrer.

Nos voisins de l'Est s'y exercent et les écoutes montrent notamment que les Allemands possèdent un réseau de T.S.F. très serré, utilisé quotidiennement pour la transmission de télégrammes chiffrés.

Si nous ne voulons pas être handicapés, il faut aussi prendre dès le temps de paix l'habitude de chiffrer.

On reproche au chiffre d'entraîner des retards dans les transmissions. Ces retards ne sont sensibles qu'avec des chiffreurs inexpérimentés.

On lui reproche aussi la complication des procédés. on a réduit cette complication au minimum compatible avec la sécurité du chiffre et compte tenu des possibilités des unités au combat. C'est ainsi que les petites unités utilisent des procédés beaucoup plus simples que les E.M. des grandes unités dotées d'un personnel spécialisé.

Au combat, les petites unités se borneront aux signaux et messages conventionnels chiffrés de l'instruction sur les liaisons et transmissions complétés par le plan de chiffrement, le carnet de chiffre ne constituant qu'un procédé de secours à n'employer qu'exceptionnellement.

La fusion du plan de chiffrement et du carnet de chiffre est à l'étude en vue de leur remplacement par un document de dimensions très réduites ne comprenant que les expressions strictement indispensables au combat et employé sans surchiffrement.

La sécurité d'un tel procédé sera recherchée dans le remplacement fréquent du document qui sera facile à reproduire et à changer.

Mais, quelle que soit la simplicité du procédé adopté, il constituera toujours une gêne. Puisqu'on ne peut s'en affranchir, il faut la rendre aussi légère que possible par un bon entraînement dès le temps de paix du personnel appelé à chiffrer (ateliers de chiffrement qui doivent fonctionner à tous les P C.)

On ne devra pas perdre de vue qu'avec les procédés de transmissions modernes, il n'est pas possible, sans chiffrer, de conserver le secret des opérations, secret qui, ainsi que le spécifie l'instruction sur le service en campagne du 10 Mai 1924"est, en toutes circonstances, d'une importance capitale".

=+=+=+=+=+=+=+=