ASSOCIATION des RESERVISTES du CHIFFRE

Nouvelle Série - N° 5 - 1977

Essai d'historique du chiffre de l'Armée de terre

6ème partie de 1945 à nos jours

Il n'a pas été possible d'écrire ici tout ce qui aurait été possible, pour une raison de discrétion que tous comprendront. Certains s'étonneront aussi de ne pas voir évoquer le chiffre en Indochine, pendant les luttes que les Armées françaises ont dû y mener pendant près de 10 ans. Cette omission est volontaire, car nous espérons pouvoir publier dans un prochain bulletin une relation détaillée, avec l'aide des principaux acteurs.

6.1 - GENERALITES

Cette sixième partie ne peut être aussi exhaustive que les précédentes, car il est évident que si les questions d'organisation peuvent être exposées au grand jour, une certaine réserve est nécessaire dans le domaine technique. Par contre, les acteurs sont pour la plupart encore présents. L'évolution du Chiffre est accélérée sous l'influence de deux facteurs essentiels : l'accroissement du volume et de l'urgence des communications à protéger, joint à leur diversification d'une part, les possibilités de calcul électromécaniques puis électroniques, de l'autre. Si ces facteurs ont conduit à la réalisation des machines automatiques complexes, ils ont conduit aussi à repenser l'organisation du Chiffre et entraîné son intégration dans les transmissions; ils conduisent aussi à la fusion de certaines tâches jadis réparties entre les états -majors, les transmissions et le Chiffre. Toutes ces transformations ne se sont pas faites et ne se continueront pas sans difficulté, car la conception des nouveaux systèmes réclame des études approfondies, comme toute mise en œuvre d'automatisation. On sait combien difficile est la mise en œuvre de la gestion automatique (informatique) dans les administrations, dans les entreprises industrielles ou commerciales; elle oblige à repenser les structures non seulement de gestion mais aussi de direction.

Le Chiffre automatique intégré aux Transmissions pose les mêmes problèmes. Son bon emploi a requis une modification profonde des relations. S'il offre un moyen adapté au commandement moderne, il réagit aussi sur les structures de celui-ci. On s'est heurté et on se heurte encore à toute l'inertie de l'homme, des structures et du budget.

Plus loin même, on peut penser aboutir à une refonte complète des modalités et des règles d'acquisition, de circulation et de traitement de l'information dans les Armées, liée à un remodelage du commandement dont on aperçoit le début dans la refonte de l'Armée de Terre qui commence en 1972.

De cela nous pouvons maintenant avoir conscience, mais il était bien difficile d'en avoir la prescience il y a trente ans et l'on comprend le désarroi de beaucoup devant des transformations nécessaires effectuées sous le coup de besoins ou de nécessités partielles dont la trame et le fil conducteur ne pouvaient apparaître. Ce sont ces transformations que les paragraphes suivants essaient de relater.

6.2 - ORGANISATION

6.2.1 — 1945 - 1951

L'organisation de 1945 reprend celle de 1939, avec deux différences :

1°) - A l'échelon interministériel existe une Direction technique des Chiffres créée le 3.8.1943 et régularisée par décret du 3.11.1945. Depuis le 7.7.1945, son chef est le Contre-Amiral Hennequin, avec comme adjoint le Capitaine Muller, qui prend sa succession le 7.1.1946. Le 21.12.1945 débute le cours de cryptographie par correspondance. Nous n'insisterons pas ici sur le développement et le rôle de cet organisme, qui deviendra en 1951 le Service Technique Central des Chiffres, puis en 1977 le Service Central des Chiffres et de la Sécurité des Télécommunications, en laissant le soin au Général Muller qui le dirigea si remarquablement, et assura la coordination interministérielle avec efficacité et la pérennité du Chiffre français pendant trente ans, de relater son évolution dans un article ultérieur.

2°) - Les Sous-officiers et les personnels féminins ont conquis et conservent le droit d'être chiffreurs ainsi même que des hommes du rang et au moins à partir de 1949, les chiffreurs apparaissent sur les T.E.D. des Transmissions (à la suite des T.E.D. homologués en A.F.N. sur le modèle des T.E.D. américains imposés pour les Troop-List).

L'annexe I, ci-jointe, donne à titre d'information les effectifs consacrés par les T.E.D. de 1949 et 1951 et ceux de la section du Chiffre de l'E.M.A. jusqu'en 1951 et du Bureau Chiffre de la D.C.T. en 1957 et 1958.

Le Chiffre vit donc une période où la direction est assumée par des organes appartenant aux états-majors et où l'exécution est confiée à des ateliers dont les personnels appartiennent, au moins dans les grandes unités à l'Arme des Transmissions, mais ces ateliers sont accolés aux centres de transmissions et relèvent des éléments de direction des Etats-Majors. Par exemple on remarque en 1948 une note du 25 février prescrivant de détacher dans les subdivisions, un sous-officier du groupe régional d'exploitation des transmissions (GRET), qui y sera chargé du Chiffre. La section du Chiffre de l'Etat-Major des Armées fournit cependant un gros travail de réorganisation et de mise en place du personnel et fait approuver un nouveau règlement du Chiffre le 31.3.1949. Mais des études sont faites dans les états-majors, en particulier aux Forces Françaises d'Allemagne, en Afrique du Nord et en Extrême-Orient sur la structure à donner au Chiffre, en particulier pour

assurer une meilleure coordination entre les trois Armées qui se posait de façon particulièrement aiguë en Indochine.

L'état-major général des Forces Armées prescrit le 18.11.1949 (N° 24/EMGFA/TRANS), la création d'une commission chargée de l'unification des règles d'organisation et de fonctionnement du Chiffre en Extrême-Orient. Les propositions de cette commission de créer un organe de direction interarmées dans le cadre du commandement des Transmissions du commandement en chef sont entérinées par décision du 28.3.1950 (108/EMGFA/TRANS du 28.3.1950). Mais le problème de l'organisation du Chiffre était posé à l'intérieur même de l'Armée de Terre et une commision créée sous la présidence du Général Babet en 1949 travailla sur le sujet pendant près de deux ans.

Les deux plus importantes questions discutées au cours de ces réunions furent les modalités :

- d'intégration des ateliers de chiffrement dans les centres de transmissions,

- l'appartenance de l'organe directeur des G.U. à l'Etat-Major (réclamée en particulier par le Lieutenant-colonel Léger dans une note du 30.11.1949) ou au commandement des Transmissions.

Le maintien de l'organe central de direction à l'E.M.A. (section Chiffre) ne fut pas mis en question.

6.2.2 - 1951 - 1957

La décision 17.587/SEFAG/CAB/EMP/OE du 24.7.1951 donna gain de cause aux partisans d'une intégration totale aux transmissions d'une part dans les centres de transmissions et d'autre part dans les commandements de transmissions des G.U. Restait à la commission à préciser les modalités d'application et malgré le combat mené par le Lieutenant-colonel Arnaud, notamment aux réunions des 6 et 7 novembre 1951, la nouvelle organisation fut mise en application par l'instruction particulière 465/SEG/CAB/EMP/OE du 8.1.1952. L'auteur du présent article, qui fit partie de la commission en question, prit le commandement des transmissions de la 6ème D.B. fin 1951. Comme initialement l'Etat-Major de cette nouvelle G.U. était un peu étoffé,

il y fut désigné aussitôt comme officier du Chiffre*, il disposait d'un sous -officier spécialiste Chiffre au titre E.M., et des chiffreurs de la compagnie puis bataillon de Transmissions. Cette fusion avant la lettre permit un passage sans heurt à la nouvelle organisation, alors que certaines difficultés apparurent dans d'autres commandements où l'officier du Chiffre n'appartenait pas à l'Arme des Transmissions.

Ce problème de personnel avait été envisagé dans l'Instruction particulière citée plus haut, qui avait prévu la possibilité de passage dans l'Arme des Transmissions des officiers spécialistes du Chiffre (active et réserve). La plupart d'entre eux acceptèrent ce changement d'Arme, mais certains préférèrent rester dans leur Arme d'origine, ce qui accrut le déficit en personnel spécialiste qui existait déjà avant la fusion, et que la section du Chiffre de l'E.M.A. combla peu à peu par des stages d'officiers.

Dans le même temps, l'instruction du Chiffre dans les Ecoles et Centres d'instruction des Transmissions fut développée et réorganisée.

Mais un autre problème d'organisation s'était posé en 1950, celui de la gestion des matériels chiffre, qui déjà avait soulevé des difficultés entre 1943 et 1945, car la M 209 était pour les Américains un matériel de transmissions, sans traitement particulier autre qu'un contrôle plus étroit des affectations. Ensuite, il se trouva que les C 36 et certaines M 209 étaient gérées par la section du Chiffre, alors que des M 209 étaient sous la responsabilité du Service du matériel.

Une décision 475/EMFGA/G/CH/3 du 2.5.1950 laissa à la section du Chiffre la gestion des machines lourdes et confia celle des machines légères au matériel, cependant la pratique fit que les machines légères furent comptabilisées et distribuées par la Section Chiffre, agissant comme détenteur dépositaire, les ateliers de chiffrement étant détenteurs secondaires (cf. règlement du Chiffre).

---

* *comme rappelé dans la précédente partie, lors du rétablissement de la 2ème R.M. en septembre 1945, il avait été nommé commandant des Transmissions de cette région et en même temps officier du Chiffre.*

Sur le plan interarmées, il y avait un officier spécialiste du Chiffre à la division transmissions de l'Etat-Major interarmées (dont la dénomination changea à plusieurs reprises), chargé de la coordination des trois Armées et des rapports avec les Alliés (OTAN en particulier). Une commission centrale des Chiffres fut créée fin 1953, pour faire progresser l'uniformisation prescrite en 1951, créer une unité de doctrine et de moyens.

A cette époque, dans l'Armée de Terre, la situation du Chiffre et des Transmissions fut codifiée dans un document règlementaire, l'Instruction provisoire sur l'emploi des Transmissions en campagne, TRS 101 qui précisait notamment la place du Chiffre dans les commandements et centres de Transmissions. Le respect des règles de sécurité du Chiffre était assuré, grâce au Général Desfemmes qui présidait le comité de rédaction et fut l'auteur principal de ce règlement.

Jusqu'en 1956, l'organisation ainsi créée se mit en place et parut satisfaisante. Il y eut cependant quelques tiraillements entre l'Etat-Major interarmées et la section du Chiffre de l'E.M.A..

Par ailleurs, l'E.M.A. ne voyait plus l'intérêt de conserver dans son sein un organisme aussi technique et spécialisé que la section du Chiffre, qui en outre augmentait son effectif, alors que le commandement recherchait des économies dans les états-majors (conséquence des évènements d'Algérie). Un incident relatif à l'emploi de certaines machines lourdes suscita de nouvelles réflexions, à l'Etat-Major interarmées, à l'E.M.A. et la question fut agitée dans le Cabinet du Ministre.

6.2.3 - 1957 et années postérieures

Une décision S/SEFAT/CAB/EMP/OE du 2.1.1957 prescrit de confier la responsabilité de la direction du Chiffre à la Direction Centrale des Transmissions et les modalités d'application parurent le 31.1.1957 par D.M. 1011/EMA/3/EPO du 31.1.1957. En conséquence, un bureau Chiffre fut créé le 1.2.1957 à la Direction Centrale des Transmissions. Le Lieutenant -Colonel des Transmissions nommé chef de ce bureau reçut heureusement tout le personnel et les moyens de la section du Chiffre de l'E.M.A., sauf son chef qui avait été muté le 31.12.1956.

Un plan de formation fut donc établi, qui reposait sur :

- la formation d'officiers du Chiffre de direction et d'exécution par des stages courts au bureau Chiffre (un stage de deux à trois semaines par an) comme précédemment à la section du Chiffre de l'E.M.A.,

- la formation d'officiers de conception, par le stage du Centre d'Etudes Cryptographiques Supérieures, créé peu auparavant par le Commandant Muller auprès du Service Technique Central des Chiffres, le besoin estimé était de un à trois par an, ces officiers pouvant obtenir le Brevet ou le Diplôme Technique. Ainsi on pouvait disposer des effectifs nécessaires pour les postes du Bureau Chiffre et du Service Central des Chiffres, les plus « mordus » ou les plus compétents pouvant y faire une bonne partie de leur carrière.

Le troisième problème était un problème bassement matériel de locaux.

Le Bureau dut quitter le boulevard Saint-Germain mais il n'y avait pas de place aux Invalides, où était alors la Direction des Transmissions. Le Bureau Chiffre fut « exilé » à la caserne de Lourcine, dans d'anciennes chambres de troupe où le volume d'air était suffisant mais où les locaux étaient incommodes et dans un état qui nécessita des travaux obtenus à grand peine.

La distance géographique entre la Direction et son bureau Chiffre ne fut pas une des moindres difficultés rencontrées pour un bon fonctionnement ! Heureusement au début de 1959, de la place fut trouvée aux Invalides auprès de la Direction, mais ce ne fut pas pour très longtemps, car la Direction dut s'installer peu après à Levallois Perret où elle se trouve encore et où le bureau Chiffre a des locaux suffisamment grands.

Simultanément s'était posé le problème de l'élément de gestion et de réparation dont l'extension était à prevoir. Après une rude bataille pour faire admettre les besoins réels présents et les extensions futures à prévoir, le Chef du Bureau Chiffre obtint, avec l'appui du directeur et du directeur-adjoint des Transmissions des locaux sinon idéals, du moins assez grands et surtout susceptibles de s'agrandir dans un des forts de la vieille ceinture de Paris.

Le quatrième problème était celui du règlement, qui était à refondre ; grâce à la parution antérieure du règlement TRS 101 mentionné plus haut, l'élaboration et l'approbation du nouveau règlement du Chiffre TRS 109 fut

assez facile. Ce règlement consacrait l'appartenance du Chiffre aux Transmissions, mais conservait l'esprit Chiffre. En même temps paraissaient d'ailleurs diverses notices sur les moyens de camouflage, dans lesquelles un certain nombre de notions issues du Chiffre purent être insérées.

Il faut d'ailleurs rendre hommage à l'esprit de collaboration et de dévouement dont fit preuve ce personnel dans des conditions difficiles. Ce passage complet aux Transmissions se heurtait en effet à des difficultés, de deux ordres :

a) - du fait des Transmissions. En effet certains officiers des Transmissions comprenaient mal la nécessité de mesures de sécurité jugées superfétatoires, considéraient certaines procédures comme des freins excessifs et auraient voulu, pour gagner du temps et des effectifs, utiliser les chiffreurs spécialistes dans d'autres emplois et banaliser les opérations de chiffrement.

La barrière de la section du Chiffre de l'E.M.A., qui maintenait les principes du règlement du Chiffre ayant sauté, il y avait à craindre des excès dangereux pour la sécurité.

b) - du fait des « vieux chiffreurs ». Ce n'était pas sans une certaine amertume que beaucoup voyaient disparaître la tête de l'organisation qui avait si bien œuvré depuis 1891, et créé un esprit de corps « sécurité » qui, des officiers d'avant 1939, s'était étendu aux sous-officiers spécialistes ; la sélection opérée par la section du Chiffre et la cooptation avaient fait d'eux des sous-officiers d'élite dont la compétence, le dévouement et la conscience professionnelle furent toujours hautement appréciés par les commandants des Transmissions.

Ainsi pouvait-on craindre certaines réticences même si officiers et sous-officiers étaient déjà intégrés dans les commandements et centres de Transmissions depuis 1951.

Surmonter ces difficultés fut le principal souci du nouveau « chef du Chiffre » qui trouva heureusement l'appui souhaitable auprès du Directeur Central des Transmissions, le Général de Corps d'Armée Marty puis le Général de Corps d'Armée Desfemmes et du directeur adjoint le Général Marcoux, dans le travail quotidien comme pour les études, les problèmes de personnel etc.... Il put aussi, pendant les deux ans et demi que dura son affectation, visiter tous les commandements des Transmissions et inspecter les

organes du Chiffre, en Europe et en Algérie et montrer ainsi que, contrairement aux craintes de certains, la sécurité n'était pas moins prise au sérieux par la D.C.T. que par la section du Chiffre de l'E.M.A..

Ainsi en 1959, étaient posées les bases d'un nouveau départ du Chiffre et ce fut la tâche des chefs successifs du Bureau Chiffre de maintenir sinon de développer, comme certains purent le faire avec bonheur mais aussi grâce à leur tenacité, l'esprit toujours vivant du vieux Chiffre, celui de sécurité, du travail bien fait et de la responsabilité. Des changements certes furent apportés, à cause de l'évolution des matériels vers un automatisme toujours plus poussé, et cela réagit en particulier sur la formation et la spécialisation des personnels.

L'automatisation du Chiffre conduisit en effet à la juxtaposition ou même à l'intégration de matériels télégraphiques et de matériels du Chiffre. Le chiffreur devenait télégraphiste, car l'exploitation de ces ensembles était purement télégraphique, avec une manœuvre supplémentaire de synchronisation.

L'ensemble d'opérations les plus courantes dans les grands centres comprenait systématiquement : régulation, perforation, transmission, incluant ou non un chiffrement automatique. Une polyvalence encore plus grande apparut nécessaire aux autorités des Transmissions et en 1971 - 1972, le remaniement des spécialités télégraphie et régulation Chiffre fut décidé et réalisé par la création des deux spécialités crypto-télégraphie et régulation-télégraphie. En 1974, ces deux spécialités furent fusionnées en une seule : crypto-régulation-télégraphie. On pourrait s'interroger sur l'efficacité réelle d'une telle mesure, car l'ensemble des matières à enseigner devenait considérable et l'on pouvait craindre que le garçon du contingent ainsi formé de façon polyvalente ne soit ni régulateur, ni chiffreur, ni télégraphiste.

Cependant, comme dans la réforme de 1958, des paliers et des passerelles furent prévus, tant pour la formation initiale du contingent et des engagés que pour la spécialisation des sous-officiers du 2ème degré.

Autant qu'on puisse en juger de l'extérieur, ces dispositions auraient apporté plus de souplesse au niveau de l'exécution tout en conservant la spécialité Chiffre des sous-officiers.

L'organisation dut donc au cours des 30 dernières années s'adapter aux besoins du commandement, profondément transformés par le fait nucléaire mais aussi au boulersement apporté dans les opérations de chiffrement par les possibilités de l'électronique.

Cependant l'évolution générale rendait urgente et critique la solution de certains problèmes d'organisation et de personnel. Le premier par son importance immédiate concernait les personnels et les spécialistes dans les centres de Transmissions. Si dans les grands centres le travail nécessitait une nette séparation des fonctions, dans les petits centres et en métropole en temps de paix, une séparation rigide des spécialités conduisait à un mauvais emploi des personnels, et la crise d'effectifs due aux opérations d'Algérie faisait qu'une certaine polyvalence était nécessaire.

L'automatisation d'autre part, dont il sera parlé dans le paragraphe suivant, allégeait le travail des chiffreurs dans une certaine mesure. Aussi à la fois pour le présent et pour l'avenir une polyvalence apparaissait nécessaire. Trois spécialités étaient voisines ou correspondaient à un travail en étroite liaison : la télégraphie, la régulation et le Chiffre. Il fut décidé, après mûre étude, de fusionner régulation et chiffre. Il était facile à un chiffreur d'apprendre la régulation. Il était possible d'apprendre le chiffre à un sous -officier régulateur. Il était par contre plus difficile de former un garçon du contingent dans la double spécialité, aussi des étapes de compétence furent prévues, les chiffreurs du contingent des transmissions recevant outre la régulation une formation simple analogue à celle des chiffreurs des corps de troupe de toutes Armes, dont la formation fut aussi réorganisée. Cette fusion n'empêchait pas, comme on l'a dit plus haut, la spécialisation et le cloisonnement (nécessaire pour la sécurité) dans les grands centres. Elle eut aussi pour résultat d'introduire plus de rigueur et d'esprit de sécurité dans les ateliers de régulation, qui en manquaient un peu parfois.

Le second fut celui de la formation des personnels (officiers) de conception et de direction, et de leur carrière. En effet comme avant la guerre de 1939 - 1945 il était impensable qu'un officier puisse faire toute sa carrière dans la spécialité pour des questions d'avancement notamment, alors que l'on avait besoin d'un assez grand nombre d'officiers compétents dans les régions, Grandes unités et centres de Transmissions, qui n'y passeraient que peu d'années et d'un petit noyau central de conception et d'exécution où un renouvellement était nécessaire.

6.3 - TECHNIQUE

6.3.1. - Mécanique et électrotechnique

La période d'avant-guerre et de guerre avait vu se développer les petites machines mécaniques (genre M 209) et les premières machines électromécaniques : B. 211 - ENIGMA - machine « pourpre » japonaise ; après 1945, les chiffreurs français « découvrirent » le téléimprimeur chiffrant allemand SIEMENS et les machines à rotors anglo-saxonnes, qui ajoutaient à un principe dérivé de l'Enigma, l'impression ou même la perforation. Le 26.6.1945, le SHAEF (haut commandement interallié en Europe), avait autorisé l'emploi « illimité » de la machine B.211. Néanmoins, la section du Chiffre de l'E.M.A. poursuivit son action dans deux directions :

- amélioration des machines existantes,

- création de machines nouvelles,

car il était évident que les machines en service n'assuraient plus une sécurité suffisante devant les perspectives du calcul électronique.

La C. 36 fut dotée de curseurs sur ses réglettes comme la M 209, de façon à changer la contexture des clés possibles et à varier celles-ci. Les deux petites machines furent, en outre vers l'année 1950, modifiées de façon à compliquer sérieusement la tâche du décrypteur, d'autant plus que cette modification fut associée à diverses améliorations de procédures.

La B. 211 fut également modifiée dans le même esprit, par l'adjonction de permutateurs changeant le tableau carré de chiffrement.

L'examen du téléimprimeur chiffrant SIEMENS avait montré l'intérêt d'une telle solution qui semblait celle de l'avenir, du point de vue de l'exploitation mais aussi la faiblesse du procédé de chiffrement, moment par moment, utilisé.

Deux études de chiffrement télégraphique automatique furent lancées, l'une par le Lieutenant-Colonel Raffalli, sur la base de cages de M 209, qui produisaient les suites nécessaires et de quelques relais de combinaison, l'autre par le Contre-Amiral Hennequin, sur la base de commutateurs téléphoniques du type R 6, agissant un peu comme des rotors. En

outre, la Marine notamment poursuivait la réalisation de translations chiffrantes dont la réalisation avait été envisagée par l'américain Vernam pendant la guerre 1914 - 1918, c'est-à-dire l'addition moment à moment d'une bande télégraphique claire à une bande télégraphique clé.

Ce procédé qui n'est autre qu'une substitution à double clé à alphabet fixe ordonné, n'était évidemment valable, comme on s'en était aperçu avec le téléimprimeur chiffrant SIEMENS, que si l'on pouvait éviter les recouvrements faciles à repérer et si le procédé de fabrication des clés de rang enlevait à celles-ci les particularités ou corrélations facilitant leur rétablissement.

Ce procédé était en fait la mécanisation des systèmes à clé additive employé dès avant la guerre et dont il est apparu au cours de la guerre qu'il pouvait assurer une sécurité parfaite dans certaines conditions.

Au début des années 1950, l'OTAN reconnut que ce système était le meilleur pour les besoins de transmission de l'époque et en décida la généralisation, d'abord avec une machine norvégienne, puis des machines italiennes etc... et la France suivit la même voie abandonnant les essais Raffalli et Hennequin au profit d'une translation télégraphique chiffrante étudiée par la société SAGEM.

Vers 1955, les moyens en service dans l'Armée française étaient les suivants :

- dans le cadre interallié :
  - machines à rotors d'origine américaine,
  - translations télégraphiques chiffrantes à bandes qui commençaient à entrer en service.

- dans le cadre national :
  - aux échelons élevés :
    - B. 211 modifiée,
    - dictionnaires avec clés-blocs.
  - aux échelons tactiques :
    - C. 36 et M. 209 modifiées,

- codes tactiques avec clés additives longues extraites de cahiers de clés,
- S.D. 43 (décrit dans la partie précédente).

6.3.2 - Electronique

6.3.2.1 - Nécessité d'évolution

Mais l'on se rendit compte à cette époque qu'un virage très important était à prendre, du fait des possibilités offertes par le calcul électronique.

Les calculateurs donnaient en effet aux décrypteurs :

- le moyen de procéder très rapidement à des recherches de corrélations, en particulier des recouvrements, et à des statistiques,
- le moyen de simuler des machines simples.

En outre, le calcul électronique permettait d'engendrer aisément des clés très variées, très longues et pseudo-aléatoires, et des systèmes de calcul complexes opérant directement sur les lettres ou les moments de l'alphabet télégraphique (algèbre de Boole). Dans ce contexte restaient seuls valables les machines à rotors et les translations télégraphiques chiffrantes à bandes d'une part, les procédés manuels à clés une fois de l'autre et des études étaient à lancer sans tarder pour remédier à la situation devenue dangereuse sur le plan de l'exploitation ; en outre, le chiffrement en ligne apparaissait un besoin du commandement pour éviter les pertes de temps et les embouteillages des ateliers de chiffrement.

Enfin, la solution des translations télégraphiques chiffrantes à bandes n'apparaissait que comme un palliatif momentané en raison des difficultés de mise en place de ces bandes et de l'impossibilité pratique de fonctionnement en réseau.

6.3.2.2 - Réalisations

Aussi fut-il décidé en France :

- de réaliser sans tarder des translations télégraphiques chiffrantes à bandes clés (matériel SAGEM), ce qui impliquait aussi la création d'ateliers de fabrication de ces bandes,
- de lancer l'étude de machines modernes, pour les petits échelons et pour le haut niveau.

Aux petits échelons, une machine électrique ou électronique ne paraissait pas souhaitable, du fait de problèmes d'alimentation, de volume et de poids, et une machine HAGELIN, dérivée de la M 209, fut adoptée. Elle présentait, par rapport à la M 209, un avantage marquant : une clé principale de beaucoup plus grande longueur, plus compliquée, rendant beaucoup plus difficile le rétablissement de celle-ci, au cas où une portion pouvait en être reconstituée par le décrypteur (recouvrements ou connaissance du clair et du chiffré). Elle fut préférée à une machine française CAMÉCA, trop encombrante et trop lourde. Pour le haut niveau une machine éléctronique permettant le fonctionnement en ligne et une synchronisation automatique était nécessaire.

Seul le principe de la substitution à double clé à alphabets incohérents pouvait être retenu, car la transposition conduisait à des retards désagréables et à des complications excessives.

Trois machines furent étudiées :

- ULYSSE
- VIOLETTE
- MYOSOTIS

ULYSSE fut écartée en raison des difficultés de fabrication en série.

MYOSOTIS, conçue par l'Armée de Terre selon un principe imaginé par l'Ingénieur d'Armement Gaubert, répondait au besoin et put même être présentée à un concours OTAN.

VIOLETTE, dont le principe avait été imaginé par le Colonel de l'Armée de l'Air Antoine, présentait l'avantage de pouvoir être compatible avec les machines à rotors alors en service et de présenter une très grande variété de systèmes de chiffrement.

Malheureusement sa présentation et sa technologie ne répondaient pas aux spécifications militaires de l'Armée de Terre et de la Marine.

Aussi MYOSOTIS fut-elle adoptée par le Ministère des Armées pour les trois Armées en 1965. Elle permettait le chiffrement télégraphique hors ligne ou en ligne à 50 - 75 - 200 - 600 - 1200 et 2400 bauds ; son degré de sécurité apparaissait pouvoir répondre à toutes les exigences.

En effet, les besoins de chiffrement de l'époque ne se limitaient pas au télégraphe classique à 50 ou même 75 bauds, mais à des besoins nouveaux de télétransmissions adaptés aux circuits P.T.T. ou radio classiques :

- transmission de données informatiques aux vitesses de 200 - 600 - 1200 ou 2400 bauds,
- transmission de fac-similé,
- transmission de téléphonie secrète après numérisation de la parole par vocodeurs

6.4 - PERSPECTIVES ACTUELLES

Comme il a été dit dans les généralités, le besoin de transmission secrète s'est étendu de l'écrit ou de la parole à tous les types d'information moderne et en particulier à l'informatique. Non seulement la nature de l'information a changé, ainsi que son volume, mais aussi, le besoin de transmission sinon immédiate du moins très rapide et aussi un besoin de stockage de l'information en sécurité. Le Chiffre électronique doit et peut répondre à ces besoins.

Il a à faire face :

- à une variété d'informations considérables, depuis la télégraphie et la téléphonie jusqu'aux données informatiques ; certaines de ces informations sont analogiques, une transformation numérique est nécessaire pour une bonne sécurité de chiffrement, de sorte que le flot d'informations à traiter peut être considéré comme du type télégraphique,

- à un volume considérable et à un besoin de transmission quasi -instantané, d'où des vitesses de transmission très grandes ;
- à l'acheminement sans retard des informations entre et vers des autorités diverses et nombreuses.

La réponse à ces deux exigences est le chiffrement de voie, c'est-à-dire la transmission continue d'informations chiffrées sur la voie de transmission équipée de modulateurs chiffrant et déchiffrant en permanence un trafic réel ou fictif,mais cette solution offre de redoutables problèmes de cheminement de l'information claire dans les nœuds, de mise à la clé et de synchronisation des dispositifs chiffrants.

A cela s'ajoute toujours le besoin de chiffrer de l'isolé ou du petit détachement qui ne peut appartenir sans cesse à un réseau permanent, ainsi que les risques de destruction, de capture ou d'intrusion de l'adversaire.

L'emploi du Chiffre déborde d'ailleurs maintenant du domaine gouvernemental, civil et militaire, dans lequel il était pratiquement cantonné depuis toujours, à cause de l'Informatique et les revues américaines techniques sont maintenant parsemées d'articles sur la sécurité en informatique et téléinformatique, qui ne peut provenir que du Chiffre.

Mais si les moyens d'exécution ont depuis 50 ans subi une mutation complète, grâce à l'Electronique le même problème de fond subsiste : assurer la sécurité de l'information stockée ou transmise. L'extension du champ d'action complique la situation, mais il est facile de se rendre compte que les besoins d'analyse de cette situation, de détermination des moyens, de définition des procédures d'emploi ont gardé les mêmes caractéristiques que jadis et réclament les mêmes qualités d'ordre, de méthode et d'imagination, auxquels doivent s'ajouter, ce qui est difficile mais non insoluble des connaissances techniques étendues.

« L'esprit du Chiffre » demeure donc et doit demeurer pour assurer la protection du secret.

ANNEXE I

TABLEAUX D'EFFECTIFS

1°) - Grandes Unités (T.E.D. Guerre)

	1949		1951 *(1)*	
	E.M.	TRS	E.M.	TRS
DI	1 + 1 + 0	0 + 1 + 9	1 + 1 + 1	1 + 20 + 11
GB	0 + 1 + 3	0 + 1 + 5		
DB	1 + 2 + 3	0 + 3 + 9	1 + 1 + 2	1 + 22 + 12
CA	2 + 3 + 5	0 + 3 + 17	1 + 1 + 2	2 + 10 + 20
GA			2 + 3 + 3	4 + 40 + 20
GAO			5 + 4 + 4	
RM			1 + 1 + 0	0 + 4 + 3

(1) - DM 8504 EMFA/G/1.O.S du 11.6.1951

1er chiffre : Officiers
2ème chiffre : Sous-officiers
3ème chiffre : Hommes du rang

2°) - Section du Chiffre de l'Etat-Major de l'Armée

Date	Section	Atelier Ch^{t} E.M.A.
26. 6.1945	8 + 6 + 3 + 12	12 + 14 + 12 + 30
19. 3.1946	7 + 9 + 2 + 8	12 + 14 + 24 + 18
8.11.1947	7 + 9 + 2 + 7	3 + 10 + 12 + 13
23. 4.1948	4 + 8 + 1 + 7	
16. 1.1950	4 + 7 + 1 + 7	

1er chiffre : Officiers
2ème chiffre : Sous-officiers
3ème chiffre : P.F.A.T.
4ème chiffre : Personnels civils

3°) - Bureau Chiffre de la Direction Centrale des Transmissions

1.2.1957 : 5 + 9 + 6 + 2 + 2 (officiers, sous-officiers, P.F.A.T., hommes du rang, P.C.)

1.1.1958 : 5 + 7 + 6 + 3 + 3 (d°)

auquel il faut ajouter à cette date l'élément chargé de la gestion et de la réparation du matériel : 2 officiers, 8 sous-officiers, 2 hommes du rang et 4 P.C..

ANNEXE II

CHEFS DU CHIFFRE DE L'ARMEE DE TERRE DE 1945 A NOS JOURS

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

Lieutenant-Colonel Léger	1. 6.1945 au 31.11.1950
Commandant puis Lieutenant-Colonel Arnaud	1.12.1950 au 31.12.1956

2 - Bureau Chiffre de la Direction Centrale des Transmissions

Lieutenant-Colonel Ribadeau Dumas	1. 2.1957 au 14. 7.1959
Lieutenant-Colonel Cullmann	15. 7.1959 au 5. 3.1961
Commandant puis Lieutenant-Colonel Jacquelin	6. 3.1961 au 24. 3.1962
Lieutenant-Colonel Samson	25. 3.1962 au 14. 1.1965
Lieutenant-Colonel de Brianson	15. 1.1965 au 14. 9.1965
Commandant Rabaud	15. 9.1965 au 10.10.1971
Lieutenant-Colonel Le Coz	11.10.1971 au 13. 8.1974
Lieutenant-Colonel Gassmann	14. 8.1974 au 31. 8.1976
Colonel Bellon	15. 9.1976 au