Histoire de la machine Myosotis

Xavier Ameil, Jean-Pierre Vasseur et Gilles Ruggiu

Association des Réservistes du Chiffre et de la Sécurité des Informations

1 Introduction

L'histoire de la cryptographie est faite d'épisodes brillants mais aussi de périodes de décadence dont la France n'est pas exempte. Les années qui ont suivi la deuxième guerre mondiale correspondent à un affaiblissement important et une inadéquation des moyens de chiffrement gouvernementaux. La plupart de ces moyens, issus de la guerre, étaient devenus particulièrement inadaptés, en raison, notamment, du développement des transmissions par téléimprimeurs.

C'est l'opération de Suez en 1956 qui en fut le révélateur et qui décida le gouvernement de l'époque à se doter de moyens modernes. C'est ainsi que fut organisé un concours entre différents industriels français sous l'égide des administrations concernées par cette technique. Il faut reconnaître que cet état de fait n'était pas propre à la France. Au même moment, la plupart des autres nations occidentales firent un constat similaire : leurs moyens de chiffrement s'avéraient de moins en moins appropriés aux besoins modernes de communication. C'est pourquoi l'OTAN lança un concours analogue.

C'est dans ce contexte que se déroula le projet Myosotis qui marqua le renouveau du Chiffre en France. Il fut d'une importance particulière pour la cryptographie française car il eut pour conséquences de :

— doter la France d'une industrie du Chiffre capable de rivaliser avec les autres grandes puissances, et de satisfaire la plupart des besoins gouvernementaux,
— définir, sous l'impulsion du Service Technique Central des Chiffres, la Doctrine du Chiffre en matière gouvernementale pour la conception, l'évaluation et l'emploi des moyens de cryptologie de l'État,
— constituer une véritable École française du Chiffre, qui perdure encore même si les structures actuelles sont bien différentes de celles de cette époque.

Myosotis est la première machine à chiffrer entièrement électronique, à base de transistors au germanium. Elle est restée en exploitation pendant plus de 20 ans.

Par sa conception, qui s'appuyait sur la meilleure approximation possible du secret parfait, elle fut certainement la meilleure machine cryptographique de son époque et on peut dire que, compte tenu de son domaine d'emploi, elle demeure la meilleure machine jamais réalisée.

2 L'état de la cryptographie en France avant Myosotis

2.1 Les administrations françaises

À cette époque, une administration civile, qu'on appelait alors les PTT (Postes, Télégraphes et Téléphones) détenait le monopole des télécommunications. Son problème était d'assurer la discrétion des liaisons téléphoniques dans, ce que l'on appellerait aujourd'hui, un souci de protection de la vie privée. Elle se souciait assez peu du secret des communications, probablement parce que celui-ci était en principe garanti par la Loi (mais la loi ne prévoyait aucune disposition technique permettant d'obtenir ce secret).

Elle avait toutefois adopté pour les liaisons radio-téléphoniques un mécanisme de protection consistant à renverser la bande de fréquences du signal de la parole (250 à 2750 Hz), via un modulateur à 3000 Hz : après filtrage, la modulation était inversée autour de la fréquence centrale 1500 Hz. C'est ce que l'on appelait le « secret international ». En cas d'interception, ce dispositif rendait la conversation inaudible (ou plutôt difficile à comprendre). Mais ce système, qui en réalité ne contenait aucun secret, était très facilement décryptable. Il suffisait de renverser à nouveau la bande.

Ce système avait donc été ensuite rendu plus compliqué en divisant cette bande en cinq parties à peu près égales et en modifiant l'ordre dans lequel se trouvaient ces cinq morceaux de bande qui pouvaient aussi être inversé. C'était le « secret à découpage de bande », conçu par la compagnie américaine Western Electric Company. Cette transformation du spectre était réalisée, de façon mécanique, au même instant aux deux extrémités de la ligne de transmission. La combinaison qui, à chaque instant, définissait ces permutations et inversions était changée périodiquement (typiquement toutes les vingt secondes) par un système mécanique à base de cames qu'un moteur électrique faisait tourner.

Ce dispositif était complexe et relativement lourd à mettre à œuvre. Cependant le secret était considéré comme faible car par une analyse de la continuité des bandes, on pouvait reconstituer le signal clair, au besoin en faisant quelques essais si des incertitudes de continuité apparaissaient.

Par ailleurs, au plan interministériel, il existait un service qui dépendait directement du Premier Ministre (par le canal du Secrétariat Général du Gouvernement) : le Service Technique Central des Chiffres (STCCh). Créé en 1951, en même temps que la Commission Interministérielle des Chiffres (CIC), il avait pour mission de

promouvoir le Chiffre français. Il supervisait au point de vue technique tout ce qui se faisait en matière de chiffrement dans toutes les administrations civiles et militaires et coordonnait leurs services du Chiffre. Structure légère d'impulsion et de coordination, le STCCh disposait de moyens très réduits : à l'origine, il n'avait qu'un chef de service, monsieur André Muller et deux adjoints. Il n'avait pas de budget pour financer des études, ni de moyens matériels modernes, à part un atelier de fabrication de bandes perforées aléatoires, créé en 1958 et installé dans la caserne du Mont Valérien. Cet atelier avait la charge d'assurer l'approvisionnement en bandes-clés « une fois » des départements ministériels qui ne voulaient ou ne pouvaient produire ces clés eux-mêmes.

Enfin, il avait été créé, sur l'initiative du Général Guérin, au sein du Comité d'action scientifique de Défense Nationale, un Centre d'Études Cryptographiques Supérieures (CECS) pour la formation de Chiffreurs de haut niveau. Le STCCh y participait ainsi que des professeurs d'Université qui deviendront d'ailleurs pour la plupart des conseillers scientifiques du STCCh. Le CECS sera rattaché au STCCh en 1962.

Le STCCh assurait le secrétariat de la Sous-Commission « Cryptologie » (cette appellation n'était pas officielle) de la CIC, dont il était l'organe permanent d'étude et de conseil. Cette Sous- Commission, sur le rapport du STCCh, donnait un avis sur la valeur cryptologique et sur l'emploi des moyens de cryptologie de l'État destinés à la protection des informations classifiées des administrations civiles et militaires.

Il est à remarquer que l'administration des PTT n'était pas représentée à la CIC. En fait cette administration affichait une certaine indifférence, voire une certaine méfiance, envers les actions de ces commissions et du STCCh, considérant sans doute que ses systèmes de secret n'étaient pas à proprement parler des machines cryptographiques. Pourtant, c'est à l'occasion de travaux de modernisation de ces systèmes que prit corps le projet Myosotis.

En ce qui concerne les administrations militaires, chaque Armée avait son propre service d'études dans le domaine des Télécommunications, à savoir :
– la SEFT (Service d'Études et de Fabrication des Transmissions) pour l'Armée de Terre,
– le STTA (Service Technique des Télécommunications de l'Air) pour l'Armée de l'Air,
– le STTM (Service Technique des Transmissions de la Marine) pour la Marine.

Enfin, l'État-Major des Armées (EMA) avait un organisme de concertation : la Commission Centrale des Transmissions (CCT), où se prenaient les grandes décisions communes aux Armées, qui devint ensuite la Commission Interarmées des Transmissions, de l'Electronique et du Chiffre (CITEC). Cette commission avait une sous-commission « Chiffre », spécifique aux Armées, et distincte de la CIC, qui, elle, re-

groupait, l'ensemble des départements civils et militaires (Affaires Étrangères, Intérieur, Colonies, SGDN, SDECE, Air, Terre, Mer, Gendarmerie, ...).

La direction de l'exploitation du Chiffre était assurée par les services « Chiffre » de chaque Armée. Pour l'Armée de l'Air et la Marine, ces services étaient rattachés aux Transmissions. Pour l'Armée de Terre, ce rattachement fut décidé en 1956 : le général Marty, Directeur Central des Transmissions fit appel au Colonel Louis Ribadeau Dumas, alors en poste à Fontainebleau, pour prendre la direction du bureau Chiffre de la Direction Centrale des Transmissions, installé aux Invalides. Il avait comme adjoint le Commandant Seyer. Félix Rabaud, Capitaine à cette époque, faisait partie de ce bureau. Au titre de ses nouvelles fonctions, Ribadeau Dumas devint membre de la Sous-Commission « Cryptologie » dont la présidence fut assurée par l'Ingénieur en Chef des Télécommunications Maurice Ollier jusqu'en 1962. Ribadeau Dumas quittera cette Sous-Commission en 1959 lorsqu'il sera nommé à Oran. Il reviendra d'Algérie en 1962, comme chef de la division Transmissions et Chiffre de l'ÉMA, et présidera la CCT.

Il n'y avait pas de compétition entre les trois Armées pour étudier et faire réaliser un matériel spécifique d'une Armée, mais des difficultés pouvaient apparaître lorsqu'il s'agissait de composants ou de matériels intéressant les trois Armées. C'était, en particulier, le cas de l'informatique qui était naissante. Aussi, en 1961, la Délégation Ministérielle de l'Armement (DMA, qui devint plus tard la DGA) a-t-elle créé un Service Central des Télécommunications et de l'Informatique (SCTI). Ce service fut chargé des études et des réalisations communes aux Armées. Plus tard, la SEFT lui sera rattachée. Le premier patron du SCTI fut l'Ingénieur Général Lacoste, qui eut pour adjoint l'Ingénieur Général Casal.

2.2 L'organisation de la CSF

Le groupe de la CSF comprenait en dehors des établissements purement CSF (rue du Maroc à Paris, Malakoff, Puteaux,...), l'ancienne SFR (Levallois, Cholet) et différentes filiales (tant en France qu'à l'étranger) qui étaient étroitement associées aux directions fonctionnelles de la CSF, voire intégrées aux groupements opérationnels correspondants.

La CSF comptait à cette époque environ vingt mille personnes et entretenait un ensemble de laboratoires de recherches de deux mille personnes, ingénieurs et techniciens : le Laboratoire de Recherches, dirigé par le grand physicien Maurice Ponte, qui succéda en 1960 à Robert Tabouis comme Président-Directeur Général de la société.

La CSF comprenait quatre grandes divisions opérationnelles :

1. Une division Matériels Professionnels, militaires et civils (Malakoff, Levallois, Cholet, Issy-les-Moulineaux) ; les études de base, par domaine, se faisaient rue du Maroc, à Levallois et au Département de Physique Appliqué installé (DPA) à Corbeville (Orsay),
2. Une division Tubes Electroniques (Levallois) avec des laboratoires d'études rue du Maroc et à Levallois, et son important centre de recherches de Corbeville : Centre de Physique Electronique et Corpusculaire (CEPEC),
3. Une division Matériels Grand Public, dérivés de l'électronique ou des techniques associées ; elle est composée essentiellement de filiales : AREL-CLARVILLE, CAMECA, SAIP-VEGA, LTI, MOP...,
4. Une division Matériaux et Composants : son laboratoire d'études était à Puteaux au Centre de Recherches Physico-Chimiques de la CSF (RPC) et sa principale usine de fabrication de semi-conducteurs était à Saint-Egrève. Elle comprenait plusieurs filiales françaises et italiennes, intégrées au groupement Composants (LCC, CICE, OREGA, COFELEC, COSEM devenue plus tard SESCOSEM...).

Les différents laboratoires de RPC étudiaient de nouveaux composants, notamment ceux à semi-conducteurs. Les travaux portaient sur les deux filières technologiques de l'époque, celle au germanium comme celle au silicium. Mais la technologie au silicium était encore expérimentale. Ces composants étaient développés dans l'usine de Saint-Egrève.

L'un de ces laboratoires avait pour objectif de promouvoir l'utilisation de ces composants à semi-conducteurs. C'est là que Jean-Pierre Vasseur, qui connaissait parfaitement leurs possibilités, disposait d'une équipe orientée dans ce sens, capable de concevoir des équipements de mesure et de nouveaux matériels utilisant ces composants.

Le directeur administratif et commercial de RPC était Xavier Ameil, qui, précisons-le pour la suite, entretenait d'excellents rapports avec l'Ingénieur Général Casal, du SCTI. Il avait la responsabilité de toutes les relations commerciales avec les Administrations pour toute la division Composants.

2.3 Les matériels cryptologiques militaires français des années cinquante

À cette époque, les machines du temps de guerre C36, M209, B211, conçues en 1935-36 par le constructeur suédois Boris Hagelin et qui avaient été adoptées par la France, étaient toujours en service dans les Armées françaises. Elles avaient été modifiées, ainsi que leurs conditions d'emploi, pour en améliorer la valeur cryptographique. Une machine électromécanique, la CX52, dont la France avait acheté la

licence de fabrication était aussi utilisée. Elle était de conception plus récente et on pouvait lui adjoindre un clavier.

On disposait en outre des machines KL-7 de l'Otan, dont la conception était différente de la famille des machines Hagelin et rappelait la machine à chiffrer allemande Enigma. De la taille d'une grosse machine à écrire (25 litres environ), elle possédait sept rotors dont deux étaient en réserve pour les rechanges. Les cinq rotors actifs avançaient tous à chaque lettre chiffrée (contrairement à l'Enigma où un seul rotor avançait d'une lettre à la fois). Son circuit électrique comprenait quatre tubes électroniques blindés : trois thyratrons et une triode. Cependant son clavier était très dur et on pouvait à peine taper plus d'une lettre par seconde. Cette machine présentait de très forts rayonnements compromettants aussi bien électromagnétiques qu'acoustiques. Bien que portable, elle n'était exploitable que dans des locaux spécialement aménagés. Il existait aussi un modèle fonctionnant sur batterie, beaucoup moins bruyant et dont les fuites électromagnétiques étaient plus faibles[1].

Ces matériels constituaient les seuls moyens mécaniques ou électromécaniques disponibles. Ils fonctionnaient uniquement en mode hors ligne.

Toutes ces machines mécanisent un procédé de substitution à double clé. Le calcul du crypto d'une lettre est défini par le carré de Vigenère : ce carré est constitué des vingt-six alphabets obtenus à partir de l'alphabet normal par un décalage de une lettre, de deux lettres, etc., comme avec le chiffre de Jules César. Pour simplifier la mécanique, les opérations de chiffrement et de déchiffrement sont identiques, c'est-à-dire que chacune de ces opérations est sa propre inverse (c'est la méthode de calcul appelée « variante allemande »).

La suite des substitutions poly-alphabétiques qu'engendrent ces machines est cependant périodique (puisque le nombre d'états de toutes ces machines est fini, ils se répètent nécessairement) et la période est plus ou moins longue : la M209 (aussi appelée Converter) a une des plus grandes périodes avec plus de 108 pas (exactement $26 \times 25 \times 23 \times 21 \times 19 \times 17 = 101405850$). Toutefois la CX52 était une machine sensiblement plus complexe que les autres, car sa loi de changement d'état était irrégulière.

Quelques années après la guerre de 39-45, un premier projet de construction d'une machine électromécanique « moderne » avait été entrepris et étudié au CNET sous l'égide d'un groupe de travail de la CIC : L'Amiral Hennequin avait conçu une nouvelle machine basée sur l'emploi de sélecteurs téléphoniques, ce qui permettait de mettre en œuvre une logique beaucoup plus riche et souple ; elle devait en principe permettre d'obtenir une vitesse de chiffrement plus élevée. Mais cette tentative

1. Malgré ses défauts la KL-7 est restée en service au sein de l'OTAN jusqu'en 1985, quand fut arrêté l'espion Walker qui vendit à l'URSS, pendant plus de 17 ans, les clés de la KL-7 utilisée par la Marine américaine.

échoua, sans doute à cause de difficultés technologiques et le projet fut abandonné. Un autre projet conduit par le Lieutenant-Colonel Raffalli, inspiré de la M209, fut aussi arrêté.

On s'orienta vers un autre système, étudié par la Marine et développé par la SAGEM : les TAREC, acronyme pour Translation Automatique Régénératrice Et Chiffrante. On savait qu'ils pouvaient assurer une grande sécurité s'ils étaient bien utilisés, et plusieurs pays de l'OTAN se mirent à en fabriquer. Les premiers TAREC ont commencé à entrer en service au milieu des années 1950. Un avantage appréciable des TAREC était de pouvoir fonctionner, au choix de l'opérateur, en ligne ou hors ligne. Ces appareils (essentiellement ceux construits par la SAGEM) se répandirent alors dans les réseaux télégraphiques des administrations civiles et militaires.

Ces machines utilisent des bandes (ou rubans) de papier perforées. Les perforations représentent des bits : un trou code un bit valant 1, l'absence d'un trou représente un 0. Chaque caractère est représenté par un ensemble de cinq perforations (puisqu'en général un caractère est codé par cinq bits pouvant ainsi fournir trente-deux combinaisons) alignées suivant une perpendiculaire à l'axe de la bande. Ces bandes sont lues (ou perforées) caractère par caractère.

Un TAREC lit simultanément deux bandes : une bande dite « clé », préparée à l'avance, et, à l'émission, la bande contenant le message télégraphique à chiffrer. Les deux caractères ainsi lus sont combinés pour produire un caractère du crypto qui est perforé sur la bande « crypto » dans les cas d'un chiffrement hors ligne ou envoyé directement en ligne dans le cas d'un chiffrement en ligne. À la réception, le caractère reçu est le crypto ; combiné avec le caractère lu sur la bande clé, il fournit le clair correspondant qui est perforé sur la bande claire.

Voici comment se présente une bande perforée :

Caractères codés	Portion de ruban
	○
U	• • ○ •
B	• ○ • •
V	• ○ • • •
Q	• • ○ •
	○

(•) = perforations, ○ - trous d'entrainement

La bande « clé » devait être aléatoire et ne pouvait être utilisée qu'une fois pour garantir la sécurité voulue : c'est pourquoi on les appelait : « /textitbandes-clés une fois », c'est-à-dire clés à usage unique *(one time pad)* en jargon anglo-américain ;

aujourd'hui, les Canadiens francophones proposent de les appeler des « masques jetables »).

Le système de calcul, identique à l'émission et à la réception, était une l'addition modulo 2 (ou addition sans retenue) bit à bit, conformément à la table suivante :

CLAIR	CLÉ	CRYPTO
0	0	0
0	1	1
1	0	1
1	1	0

Ces machines ne sont pas à proprement parler des machines à chiffrer, mais de simples additionneurs (modulo 2) munis de lecteurs-perforateurs de bandes. Cependant ces systèmes sont théoriquement indécryptables à condition toutefois que l'aléa des bandes-clés soit de grande qualité et que chaque bande-clé ne soit utilisée rigoureusement qu'une seule fois[2]. Si la première condition est relativement aisée à satisfaire par l'utilisation d'un ensemble de tests adéquats, en revanche la seconde qui est de nature organisationnelle est très difficile à appliquer et à vérifier. Elles constituent des exemples de machines à secret parfait.

Cela ne signifie pas pour autant que ces machines basées sur des clés à usage unique soient inattaquables ! Bien au contraire, une mauvaise utilisation des clés peut anéantir toute leur sécurité[3]. De plus, les lecteurs-perforateurs de rubans, par

2. Si ces bandes sont utilisées plus d'une fois, c'est toute la sécurité du système qui est compromise. Cette contrainte est cependant difficile à respecter, souvent à cause d'incidents se produisant lors de la préparation ou de la transmission des messages, mais aussi d'erreurs des opérateurs. L'anecdote suivante est révélatrice de ce genre de difficultés.
En 1968, A. Muller décida de doubler le prix des bandes aléatoires qu'il fabriquait pour les différents organismes gouvernementaux. Il les vendait, jusqu'alors, à un prix dérisoire, très nettement en dessous de leur prix de revient. Cependant un Général, responsable des transmissions d'une des Armées, refusa de doubler le budget correspondant. Il semble bien qu'il soupçonnait le STCCh d'avoir « inventé » la règle d'utilisation unique des bandes pour pouvoir en vendre plus ! Il ordonna à son chef du bureau Chiffre de commander la moitié des bandes dont il avait besoin, en lui donnant la consigne d'utiliser les bandes deux fois. Ce dernier expliqua, en vain, qu'une telle procédure était très dangereuse. Et il fallut l'intervention des plus hautes autorités du Chiffre pour faire revenir le Général sur sa décision.

3. Voir par exemple l'article de L. Ribadeau Dumas, « Le Projet Venona »,*Bulletin de l'ARCSI*, n° 25, p. 77-81. Ce projet Venona est une claire illustration de l'écart existant entre la sécurité théorique (ici, le secret parfait), prouvée mathématiquement, et la sécurité pratique correspondant aux conditions réelles d'utilisation. En effet, il est impossible de démontrer que les hypothèses de la preuve mathématique, qui sont de nature abstraite, sont en complète adéquation avec la mise en œuvre réelle du système de chiffrement, qui, elle, est de nature concrète. On ne peut que se contenter de vérifier expérimentalement que cette adéquation n'est pas ouvertement contredite par les faits.

les forts appels de courant qu'exige leur fonctionnement, présentent un rayonnement électromagnétique élevé qui peut compromettre gravement la confidentialité des informations traitées.

Ces TAREC permettaient d'accélérer les opérations de chiffrement, mais la production des « *bandes-clés une fois* » et leur mise en place auprès des ateliers de chiffrement exige une logistique très lourde. Par ailleurs l'inconvénient du TAREC apparaît évident quand on constate qu'il interdit de travailler en réseau sous peine de voir la sécurité du chiffrement s'effondrer, sauf pour les réseaux en étoile, organisés autour d'un centre émetteur-récepteur travaillant avec les autres destinataires qui ne correspondent pas entre eux. La structure des réseaux des Ministères de l'Intérieur ou des Affaires Etrangères est typiquement en étoile (les Ambassadeurs comme les Préfets ne correspondent pas entre eux).

Il faut noter que la distribution des bandes-clés, assurée par les organismes de gestion du Chiffre des départements ministériels, exige un canal sûr dont la capacité de transmission soit au moins égale à celle du canal normal de communication, lequel, par hypothèse, n'est pas sûr (puisque les clés doivent être aussi longues que les clairs). Le seul paramètre qui distingue ce canal sûr du canal ordinaire non sûr est le temps : on choisit le moment de transporter les bandes et on se donne le délai nécessaire correspondant au moyen de transport adopté. C'est ce degré de liberté, offert par le paramètre temps, qui permet de sécuriser ce canal, contrairement au canal de communication ordinaire.

Mais, la nécessité d'accélérer les opérations de chiffrement et l'existence sur le marché de téléimprimeurs chiffrants, permettant de réaliser simultanément les opérations de chiffrement et de transmission (téléimprimeurs chiffrants Olivetti ou Siemens, dont le T52 fut facilement décrypté par les Suédois, translations chiffrantes Lorenz, beaucoup plus solides ou les T-52 et T-55 d'Hagelin), commandaient de s'orienter vers le chiffrement télégraphique automatique.

2.4 La situation défavorable du chiffre français à cette époque

Il faut reconnaître que, dès cette époque, toutes ces machines (hormis les TAREC et la KL-7) sont d'une conception ancienne et leur sécurité cryptologique était toute relative. Par exemple la M209, malgré sa grande période, ne pouvait assurer le secret que pendant quelques heures et son utilisation était limitée aux communications tactiques de bas niveau de confidentialité. Faute de crédits pour financer des études, on se contentait de rechercher sur le marché les matériels qu'offraient les industriels. Ceux-ci proposaient en général des modèles ayant des possibilités de modifications afin de les personnaliser en fonction du client. L'EMA examinait ces possibilités et demandait au constructeur d'apporter aux machines achetées les modifications choisies.

En fait, il est triste de constater que la conception de ces machines, c'est-à-dire les travaux qui relevaient de la « défense », n'avaient pas bénéficié des progrès techniques et scientifiques de l'époque et notamment de ceux réalisés au cours de la seconde guerre mondiale, alors que la cryptanalyse et, plus généralement, toutes les techniques et procédés relevant de « l'attaque », s'étaient considérablement perfectionnés, tant dans leurs méthodes que dans leurs outils.

En France, tout en sachant qu'il convenait de moderniser ces moyens, on semblait cependant s'en accommoder, car on ne soupçonnait pas ces énormes progrès. Les extraordinaires décryptements réalisés en Angleterre, à Bletchley Park lors du conflit de 39-45 restèrent longtemps secrets et ignorés des hauts responsables civils et militaires français. En particulier, les décryptements de la machine allemande Enigma, qui ont entraîné la construction de ces machines spéciales baptisées « les Bombes », et où s'illustra le grand mathématicien et logicien britannique Alan Turing, ne furent révélés qu'à partir de 1973.

Une autre avancée technologique considérable avait été réalisée par les Américains avec le système de cryptophonie digitale SIGSALY. Il était basé sur le vocodeur mis au point, dès 1939, par les Bell Telephone Laboratories et fonctionnant à 1800 bits/seconde. L'équipement correspondant pesait 55 tonnes. Ce système, mis en service en juillet 1943, fut tenu secret jusqu'en 1976 !

L'arrivée des ordinateurs ne pouvait qu'aggraver la situation. Ainsi, on considère aujourd'hui, mais on l'ignorait dans les années cinquante, que le premier ordinateur électronique (programmable) fut la machine Colossus, construite à des fins cryptologiques par les Britanniques en 1943 (de mars à décembre).

Les premiers ordinateurs de la fin des années cinquante étaient incomparablement plus puissants que Colossus, tant en ce qui concerne la vitesse de calcul que la capacité de la mémoire. Ils étaient déjà beaucoup plus facilement programmables. Ainsi La NSA *(National Security Agency)* américaine s'équipe en 1962 du calculateur le plus puissant du monde du moment : le « Stretch » (dont le nom commercial fut 7030) de la compagnie IBM. Ce calculateur pilotait un système de stockage des informations sur bandes magnétiques de 88 milliards de caractères sur 160 bandes (le système « Tractor »). Enfin sont mis au point de nouveaux langages de programmation et de nouveaux systèmes d'exploitation qui, en créant l'industrie du logiciel, ouvrent de nouvelles perspectives en matière d'algorithmique : les méthodes de cryptanalyse les plus complexes et les plus subtiles pouvaient enfin être automatisées et appliquées à des masses de données considérables et ce, dans des temps extrêmement courts.

On sait que, durant la deuxième guerre mondiale et malgré les vicissitudes de la situation de la France, les services français réalisèrent, avec les moyens du bord, de nombreux décryptements et, en outre, contribuèrent grandement, par les ren-

seignements fournis, aux décryptements britanniques de l'Enigma[4]. Mais ils furent tenus à l'écart des travaux qui se faisaient à Bletchley Park, dont ils ignorèrent tout : les quelques Français ayant collaboré à Bletchley Park se turent aussi jusqu'en 1973. Les services français n'eurent donc pas l'occasion de se familiariser avec ces nouvelles techniques ni même d'en présumer la valeur. Cette situation était d'autant plus défavorable pour le Chiffre français que les militaires considéraient que le Chiffre ne servait qu'à ralentir les transmissions (on avait encore le souvenir de la campagne de mai-juin 1940) !

3 La conception de Myosotis, le concours national et le concours OTAN

3.1 Les prémices du concours interne français

L'intervention franco-britannique de Suez, en 1956, avait mis en évidence l'inadéquation de nos moyens de chiffrement, tant nationaux que OTAN. Nos alliés britanniques nous firent savoir qu'il ne fallait plus utiliser la B211 qui devait être considérée comme périmée ; en outre les délais de chiffrement et de déchiffrement étaient apparus largement excessifs. Cela fut un choc considérable pour les militaires. On décida de retirer la B211 des services et d'utiliser à la place la KL-7 qui est alors fournie aux Armées, dans le cadre de l'OTAN.

Sous l'impulsion d'André Muller, les autorités gouvernementales décidèrent de rénover nos moyens de chiffrement. Un plan de modernisation des équipements fut lancé et approuvé en 1957 par la CIC. Des crédits furent débloqués aux Armées. On acheta d'abord la licence de fabrication de la CX52. Puis on s'orienta vers la conception d'une nouvelle machine et la décision de lancer l'étude d'une machine à chiffrer télégraphique fut prise.

Les trois Armées voulaient chacune en faire une et une véritable guerre des « boutons cryptologiques »commença. La Marine entrepris d'étudier la machine « Ulysse »à laquelle allait collaborer la SEA, la compagnie d'informatique créée par François-Henri Raymond, connue pour les ordinateurs originaux qu'elle fabriquait. L'Armée de l'Air, avec principalement le Colonel Antoine, se lança dans la conception d'une machine à partir de la KL-7 ; celle-ci est devenue « Violette »et a été étudiée par la SAGEM.

Mais c'est Marius Gaubert, représentant la SEFT à la Sous-Commission « Cryptologie » qui, vers la fin de l'année 1958 ou le tout début de 1959, soumet une idée

4. Il semble que, sur une initiative du Général Colson, chef d'État-Major des Armées, des travaux analogues à ceux de Bletchley Park aient eu lieu en France, dans les premières années de la guerre, au sein de la compagnie des machines Bull pour décrypter l'Enigma (cf. l'article paru dans le numéro 23 (1995/96), p. 41 du *Bulletin de l'ARCSI*).

vraiment originale. Celle-ci consiste à effectuer le calcul du crypto en tirant des alphabets aléatoires[5]. Cette idée est discutée par la Sous-Commission qui, naturellement, la trouve très intéressante. Mais si, sur le plan théorique cette idée est séduisante, encore faut-il démontrer, d'une part, qu'un tel organe de calcul, capable de fonctionner avec la vitesse voulue est réalisable, d'autre part, que l'on sait faire un générateur d'aléa capable de fournir les suites de lettres nécessaires pour constituer les alphabets aléatoires. Ce générateur d'aléa devait offrir un haut niveau de résistance aux attaques cryptographiques connues tout en respectant les exigences du trafic envisagé pour cette machine ! En l'occurrence, il s'agissait d'un générateur pseudo-aléatoire, puisque le destinataire devait pouvoir fabriquer les mêmes alphabets aléatoires pour déchiffrer les messages.

C'est le colonel Ribadeau Dumas qui s'attaque, au début de 1959, à la première condition de faisabilité : il s'agit de déterminer le nombre de tirages minimum permettant d'obtenir, avec une bonne probabilité, les alphabets voulus, sachant qu'il fallait envisager des alphabets à 26, 27, 31 ou 32 lettres. Ribadeau Dumas aboutit à des formules très compliquées à calculer numériquement, surtout à l'époque où l'on ne disposait pratiquement pas d'ordinateurs et où les machines à calculer étaient très rudimentaires. La principale difficulté était de devoir effectuer énormément de calculs avec une très grande précision, car il fallait soustraire de très grands nombres dont les valeurs étaient très voisines. Ribadeau Dumas réussit à définir des conditions d'approximation et les formules approchées correspondantes. Il parvint à effectuer une première série de calculs permettant de déterminer les longueurs de tirages nécessaires. Ainsi dans le cas d'un alphabet de 31 lettres (le 32^{e} caractère n'étant pas utilisé en télégraphie), il trouve qu'il faut 127 tirages pour obtenir un alphabet complet avec une probabilité d'environ 90%.

Une première condition que doit satisfaire la machine est ainsi établie. Si le résultat obtenu par Ribadeau Dumas ne paraît pas incompatible avec la technologie de l'époque, on est encore loin de la définition d'une machine à chiffrer et de la preuve de sa faisabilité !

Partant à Oran, Ribadeau Dumas arrête là ses travaux. À son retour en 1962, la machine Myosotis est déjà bien avancée. André Muller lui demandera tout de même de revenir à la Sous-Commission « Cryptologie », où il participera à la suite des travaux et surtout à la décision finale.

5. Il semblerait que l'idée de tirer un alphabet aléatoire pour traiter chaque lettre ait germée au CECS parmi les stagiaires, mais on ne savait pas comment la réaliser. L'idée aurait été exposée à M. Gaubert qui a su la mettre en pratique par le mécanisme du chiffrement à la volée !

3.2 Les premiers contacts de la CSF avec le chiffre

En 1959, le commercial de la CSF, chargé de l'Armée de Terre, M. Moineau, camarade de promotion de l'École Polytechnique du directeur de la SEFT, l'Ingénieur Général Revirieux, apprend par ce dernier que la SEFT voulait transistoriser le système mécanique permettant le brouillage des communications hertziennes selon le principe du découpage de bande dont on a parlé plus haut. En fait, il s'agissait d'un matériel de cryptophonie à 4 bandes, le DT414, développé par l'Armée de Terre, était piloté par un système mécanique de la société CAMECA.

M. Moineau avertit Xavier Ameil. Celui-ci organise la première relation technique entre l'Ingénieur en Chef Gaubert, chargé du projet au sein de la SEFT, et le spécialiste des études de transistorisation Jean-Pierre Vasseur. Le projet prend corps. Ce travail est réalisé dans le cadre d'un marché passé au centre de Levallois et un prototype est réalisé. C'est en fait, pour Jean-Pierre Vasseur, l'occasion de commencer à réfléchir à ce que pourrait être une machine à chiffrer électronique.

Il a alors la possibilité de développer ses idées quand, pendant l'été 1960, la SEFT propose à RPC de mettre au point une maquette d'un équipement de chiffrement de fac-similé, ceci dans le cadre d'un contrat de l'Armée de Terre avec les États-Unis. RPC répond positivement et J.-P. Vasseur en est chargé. Une équipe est constituée et les principaux responsables de la réalisation sont Jacques Riethmüller, spécialiste de l'électronique, et Marc Dumaire qui est embauché à RPC à cette occasion, en septembre 1960. Il apporte, en particulier, sa compétence dans la conception des circuits logiques. Marc Dumaire venait de la SEA, impliquée aussi dans le chiffre avec la machine Ulysse, mais à laquelle il n'y avait pas pris part.

Dans ce projet de chiffrement de fac-similé, si la synchronisation de la liaison fax était un des points délicats à résoudre (il faut en particulier définir avec précision le point de départ du message) les algorithmes nécessaires au chiffrement retiennent l'attention de J.-P. Vasseur qui voyait là une étude particulièrement fertile pour la suite. Il a d'ailleurs l'occasion de constater qu'en dépit d'une algorithmique très élaborée, mise en œuvre par une électronique complexe, on pouvait obtenir des fax chiffrés qui laissaient deviner certains éléments du clair ! En effet, les images sont extrêmement redondantes et l'information qu'elles contiennent est très difficile à masquer. C'est par une analyse statistique poussée que l'on a pu mettre en évidence l'origine du défaut et apporter la correction correspondante.

3.3 Le début de l'affaire Myosotis

C'est au cours de ces premiers travaux que Marius Gaubert et Jean-Pierre Vasseur en viennent rapidement à parler des machines mécaniques de chiffrement existant alors (ou de nouvelles à concevoir ?) et de leur éventuelle transistorisation. Qui en

a eu le premier l'idée : Gaubert, Vasseur... ou les deux ? Et surtout ils discutent de l'idée du tirage des alphabets aléatoires. Beaucoup de problèmes restaient à régler, en particulier celui de compléter l'alphabet quand la suite des tirages n'a pas fourni toutes les lettres voulues, sans en détruire le caractère aléatoire.

La force de l'idée de Gaubert, c'était de pouvoir effectuer le chiffrement à la volée, sans avoir à mémoriser l'alphabet chiffrant. Marius Gaubert dépose un brevet le 1er Août 1960 (brevet n° 834596). L'évolution de l'électronique que l'on pressentait déjà permettait d'espérer que ce principe pouvait être rendu compatible avec les exigences de vitesse des transmissions télégraphiques (50 et 75 bauds). Jean-Pierre Vasseur a immédiatement vu un grand intérêt dans ce brevet, surtout si on pouvait le coupler avec le système de génération de clé auquel il réfléchissait. L'idée de construire un prototype d'évaluation prend corps.

Quel qu'en soit l'initiateur, le fait important est que RPC a pris la décision d'étudier et de réaliser sur fonds propres un tel prototype, décision qui n'avait pas la totale bénédiction du directeur technique du laboratoire, Claude Dugas, qui pensait, à juste titre, qu'un laboratoire de composants n'est pas destiné à étudier et réaliser des prototypes de matériels.

Par ailleurs, l'OTAN lançait à ce moment un concours pour réaliser une machine cryptographique pour la télégraphique et dont l'échéance de présentation était février 1963.

L'équipe de Vasseur travaille donc d'arrache-pied car le délai de présentation à l'OTAN est très court. Deux maquettes de démonstration en valise sont réalisées pour une présentation aux Armées, dans le bureau de M. André Danzin, Directeur du groupement Matériaux et Composants.

Ces maquettes mettent déjà en évidence les points forts de Myosotis. Une des caractéristiques importantes de Myosotis était son système de mise à la clé du jour : Vasseur en inventant les permutateurs enfichables réalisait un progrès considérable par rapport aux systèmes utilisant des câbles enfichables :ils se sont révélés plus fiables et plus faciles à utiliser. Ils permettaient de définir un très grand nombre de clés : le nombre de clés de Myosotis était 10000 fois plus grand que celui de la KW-7. Cependant ils furent le prétexte de nombreuses critiques de la part des Anglo-Saxons lors du concours OTAN.

Autour de l'idée des permutateurs, Vasseur applique plusieurs principes fondamentaux, souvent inspirés de la théorie de Shannon :
– introduire des circuits non linéaires,
– obtenir l'équiprobabilité des variables binaires internes,
– casser les corrélations entre ces variables en les rendant statistiquement inexploitables,
– créer de la confusion et de la diffusion entre les informations,

– introduire le maximum d'ambiguïté entre les informations internes de la machine et le crypto.

La fréquence d'horloge choisie est aussi élevée que possible pour pouvoir atteindre les plus haut débits de cette époque (2400 bits/s). Mais ceci pose des problèmes complexes de consommation et d'échauffement, d'autant plus difficiles à résoudre que les contraintes d'ambiance imposées par les Armées sont sévères.

Enfin, Vasseur pense à tous les mécanismes auxiliaires nécessaires pour faciliter le travail des opérateurs et diminuer les risques d'erreur : mise en opération, synchronisation, détection des pannes, alarmes, maintenance.

Dés que les premiers résultats sont prometteurs, J.-P. Vasseur et X. Ameil, accompagnés de Jean-Charles Devin, PDG de LCC et chargé des problèmes internationaux pour la division Composants, demandent audience au PDG de la CSF, Maurice Ponte. Il faut, en effet, le mettre au courant de cette affaire et qu'il veuille bien approuver cette décision. L'argument majeur présenté est que le délai de réalisation d'un prototype de machine est si court qu'il est pratiquement impossible de le faire réaliser par une équipe de matériel, peu habituée aux possibilités des semiconducteurs et surtout ne connaissant pas intimement l'Ingénieur en Chef Gaubert dont la collaboration était indispensable. À l'issue de l'entretien Monsieur Ponte donne son accord avec un crédit exceptionnel d'études internes. C'est sur ces crédits que le projet Myosotis a été lancé.

Il est décidé que J.-P. Vasseur rapporterait directement à M. Ponte pour la suite des travaux.

De son côté, Maurice Ponte se charge de calmer les dirigeants de la division Matériels. En effet, ceux-ci voyaient d'un mauvais œil le fait de ne pas être dans le coup dès le départ dans le futur marché de la cryptographie qui était seule envisagée, au premier abord. Mais, en fait, les matériels prototypes ont tout de même été réalisés avec les moyens de Levallois.

Il faut dire que Maurice Ponte avait tout de suite compris l'intérêt du secret pour une compagnie dont une des activités principales était la communication par radio. En outre, il s'intéressait beaucoup à la technique et visitait le laboratoire environ deux fois par mois. J.-P. Vasseur allait lui rendre compte assez souvent dans son bureau. Son appui personnel a été déterminant dans le succès de Myosotis.

3.4 Le lancement du concours OTAN

Le Comité Militaire de l'OTAN avait lancé un appel à candidature pour une machine à chiffrer télégraphique électronique, sur la base de spécifications définies par l'ACSA *(Allied Communications Security Agency)*. Il était précisé, entre autres, que la machine devait être sans bande, ni rotor *(tapeless and rotorless)*, donc pas de

systèmes utilisant des « bandes-clés une fois », ni de machines électromécaniques dérivées de l'Enigma, comme la KL-7.

Elle devait avoir les deux modes de fonctionnement : en ligne ou hors ligne. En outre, l'ensemble de la station de chiffrement devait répondre à des contraintes très sévères concernant le rayonnement et la conduction électromagnétique des circuits véhiculant des informations claires traitées par la machine (contrainte TEMPEST : *Transcient ElectroMagnetic Pulse Emanation Standard*). Le problème du rayonnement avait été posé au début des années cinquante par une machine à bande aléatoire dont les relais provoquaient un très fort rayonnement dans lequel on pouvait retrouver des informations claires. Il semble que les Américains avaient appris que ce phénomène avait été exploité à Moscou au détriment de leur Ambassade. Le cahier des charges indiquait simplement « aucun rayonnement détectable », sans préciser les conditions de mesure !

Il faut ajouter que le cahier des charges original, rédigé en anglais, mais mal traduit en français, a été, sur plusieurs points, mal compris, et notamment sur l'aspect opérationnel. Heureusement, le Commandant Rabaud, fort de son expérience de l'exploitation, a su définir les modifications à apporter au bloc de commande de Myosotis pour être conforme aux exigences OTAN.

La technologie électronique en circuits discrets de l'époque et les transistors, qui venaient d'être inventés (1948), allaient permettre une souplesse et une complexité de conception cryptologique jamais atteinte par la technologie électromécanique antérieure. En outre, une rapidité de traitement supérieure aux vitesses télégraphiques usuelles était envisageable : le sempiternel reproche de lenteur fait au Chiffre allait enfin tomber ! Il est vrai que l'électronique des années cinquante utilisait presque exclusivement des lampes (tubes à vide : diodes triodes, pentodes...). Mais le nombre de circuits nécessaires rendait la réalisation d'une machine à chiffrer à lampes totalement irréaliste. Il était temps de songer à recourir à l'électronique des composants solides, celle des semi-conducteurs, pour réaliser de nouvelles machines.

Il s'agissait non seulement d'améliorer les qualités cryptographiques de ces machines, mais aussi leurs conditions d'utilisation en automatisant plus de fonctions dans un volume plus faible et en les rendant plus maniables pour réduire les erreurs d'exploitation. En outre, l'électronique à semi-conducteur diminuait considérablement le poids, l'encombrement et la consommation, donc l'alimentation. Ceci allait dans le sens d'un élargissement du domaine d'emploi des machines, surtout pour les besoins tactiques, et permettait d'envisager des systèmes embarqués ou portables. Il fallait aussi satisfaire les nouvelles exigences des télécommunications, en particulier l'augmentation de la vitesse de transmission.

La Défense décide de répondre et de participer à ce qu'on appellera le « concours OTAN », puisque d'autres pays vont aussi présenter leurs matériels.

3.5 Les machines étrangères concurrentes de Myosotis

Trois autres pays ont participé au concours OTAN : les USA, qui présentaient la machine KW-7 ; le Royaume Uni, la machine ALVIS ; et l'Allemagne, l'ELCROTEL.

La KW-7 était entièrement transistorisée. Sa logique était plus simple que celle de Myosotis et l'aléa qu'elle produisait était certainement de moins bonne qualité en raison de la présence de corrélations temporelles assez évidentes. Mais surtout le calcul du crypto était beaucoup plus rudimentaire : c'était une simple addition modulo 2, bit à bit. Ce calcul était donc très sensible aux attaques basées sur les messages parallèles, bien qu'il utilisât un dispositif d'autoclave par caractère (sur cinq bits).

Mais le principal avantage de la KW-7 était l'utilisation d'un registre R linéaire et à période maximale, dont la structure était définie par un polynôme primitif de degré 39. Ce registre comportait donc 39 pas et avait un avancement irrégulier. Il assurait une période minimale importante : $6,87.10^{11}$ environ, plus grande que celle de Myosotis ($3,2.10^{9}$). Cependant la période moyenne de la KW-7 ($5,5.10^{12}$, environ) était comparable à celle de Myosotis (3.10^{12}).

La mise à la clé du jour de la KW-7 consistait à connecter trente entrées de portes logiques avec les trente et un premiers étages du registre R. En admettant que toutes ces combinaisons définissent autant de configurations distinctes, cela représente un nombre total de clés de :

$$K = 31! = 8,2.10^{33}$$

La KW-7 pesait à peu près 40 kg pour un volume de 50 litres était comparable à Myosotis (cf. le paragraphe 4.1). Elle a été construite selon deux variantes dont les mises à la clé étaient différentes. Dans la première, on établissait les connexions manuellement avec des câbles que l'on enfichait dans des prises sur un tableau de branchement. Ce système, assez archaïque et rappelant étrangement l'Enigma, était d'une mise en œuvre assez pénible et sujette à l'erreur. La deuxième variante utilisait des cartes perforées inspirées des machines IBM. Ce système était plus commode mais nécessitait un matériel spécial de perforation pour préparer les cartes. Ces deux variantes n'étaient pas compatibles et ne pouvaient communiquer entre elles ! La Marine américaine adopta la variante à cartes perforées, tandis que l'Armée de Terre adopta la machine à câbles. La KW-7 resta en fonction jusqu'en 1988.

L'exploitation et surtout la maintenance de la KW-7 étaient assez laborieuses, car la détection des pannes était très difficile. Cette machine exigeait un à deux mois de formation. Sa principale protection contre les indiscrétions était un capot dont le verrou se manœuvrait à l'aide d'une clé plate. Pour des raisons de sécurité, celle-ci était très difficile à reproduire car elle comportait trois rangées de dents (une rangée d'un côté et deux de l'autre).

La machine ALVIS aussi utilisait un registre linéaire à période maximale. Mais le reste de la logique était relativement peu complexe et on peut s'interroger sur sa valeur cryptologique. La taille de la machine était impressionnante : c'était une baie d'environ deux mètres de haut et soixante centimètres de large, contenant six gros tiroirs d'électronique. La mise à la clé du jour de la machine consistait à configurer un tableau de branchements. Cette configuration était réalisée par deux cartes de circuits imprimés (d'environ 8 cm sur 12) que l'on introduisait dans des connecteurs. Ces cartes contenaient trente câbles soudés sur une rangée du bas ; ces câbles devaient être enfichés dans des prises situées sur ces cartes dans trois rangées au-dessus. Ces cartes pouvaient être préparées à l'avance mais elles étaient relativement fragiles et sujettes à de nombreuses pannes (coupures ou mauvais contacts des câbles).

Quant à la machine allemande, nous n'avons pas eu beaucoup d'informations sur elle. Il semble que sa logique présentait quelques similitudes avec celle de Myosotis. Sa mémoire était une matrice de tores de ferrite. Mais c'était une machine volumineuse et son bloc de commande était une fois et demi plus gros que le bloc de chiffrement. Comme sa fréquence de fonctionnement était relativement élevée pour l'époque : 500 kHz, on a pu, par la suite, en faire une version, appelée ELCROVOX, adaptée à la cryptophonie grâce à un vocodeur fonctionnant à 2400 bits/s.

3.6 La présentation de Myosotis au concours OTAN

C'est donc en 1961 que la CSF, en accord avec le SEFT et pour le compte de l'Armée de Terre, se lance dans ce concours, en troisième position car il y avait déjà deux autres projets en lice : les machines Ulysse de la SEA et Violette de la SAGEM. Mais, finalement, seule Myosotis sera présentée au concours OTAN.

Le concours OTAN comportait trois phases : un examen au SHAPE à Rocquencourt, des essais opérationnels dans l'air, sur mer et sur terre, et enfin une évaluation cryptologique à Washington.

Le délai de février 1963 imposait une équipe solide et performante pour réaliser en moins de dix-huit mois les trois prototypes destinés à être testés dans les conditions opérationnelles par les différentes Armées. Il fallait donc un appui industriel que Vasseur trouva auprès du centre de Levallois, centre que, par ailleurs, il connaissait bien pour y avoir fait ses débuts à la CSF.

Le service de Levallois met alors en place une équipe ayant déjà l'expérience du DT 414. Cette équipe, placée sous la responsabilité de la direction des études, est menée par MM. Seignol et Samain. Ils surent allier organisation et savoir-faire technique avec le responsable du développement et le bureau d'étude pour réussir à sortir le matériel en moins d'un an.

En février 1963, c'est la présentation au SHAPE. Le matériel, officiellement présenté par l'armée française, avait été transporté sous escorte militaire. Les clés, qui avaient été faites par Rabaud, furent scellées dans des enveloppes opaques aux rayons X. Comme pour les autres concurrents, à Rocquencourt, il y eut une première série d'examens par les services américains. On se rendit compte que le concours était très partial. Par exemple, une panne se produisit et fut vite réparée. Mais la délégation anglaise en a aussitôt profité pour demander l'élimination de Myosotis. Les Français durent faire appel ; la demande anglaise fut âprement discutée et finalement elle fut tout de même refusée : Myosotis restait en course !

Les Anglo-Saxons, qui préféraient les câbles aux permutateurs (sans doute parce qu'ils n'en avaient pas eu l'idée !), émirent à leur encontre des critiques injustifiées :

— ils les assimilaient à des rotors, alors que leur rôle était très différent (ils ne tournaient pas et associés aux codeurs et aux décodeurs, ils introduisaient une fonction non linéaire d'une très grande force cryptographique),
— ils soulignaient qu'ils pouvaient être capturés et donc pouvaient compromettre la sécurité de Myosotis, alors que celle-ci ne reposait nullement sur le secret des permutateurs !

En mars, le matériel est expédié pour procéder aux essais opérationnels : aéroportés, embarqués sur deux bateaux de la Marine américaine et sur une station terre à Malte. Les essais aéroportés furent organisés à partir de la base américaine d'Evreux, sous le contrôle du Silk Purse Control Group, qui constituait le PC volant de l'US Air Force en Europe. Côté français, le responsable était le Commandant Christian Fabre de la Base Aérienne 134. Son interlocuteur principal était le Major Cooper qui lui servait en même temps d'interprète.

Les essais se sont étalés sur une période de deux mois. Les vols, qui se déroulaient sur un quadrimoteur du type DC7, duraient 12 heures, mais seule une demi-heure était vraiment opérationnelle. Ils consistaient à survoler la Champagne. La base d'Evreux était assez souvent sujette au brouillard : plusieurs atterrissages ont été plus qu'acrobatiques et une fois l'avion a dû être détourné sur la base américaine de Torrejón en Espagne ! Les essais concernaient Myosotis et la KW-7 qui était embarquée sur le même avion. Ils étaient réalisés par une équipe américaine composée de deux officiers supérieurs et d'un sous-officier. Ils opéraient dans une zone centrale de l'avion équipée de moyens de télécommunications, où ils communiquaient avec Malte, mais où les Français n'avaient pas le droit d'aller.

La principale difficulté de ces essais était la transmission des clés, car les Français, qui n'avaient pas eu le temps de s'y préparer, n'avaient pris aucune précaution contre d'éventuels problèmes de communication. Or la liaison s'est révélée très défectueuse et cela entraîna beaucoup d'erreurs de transmissions, donc des clés erronées, qui ont dû être retransmises plusieurs fois. En revanche, les Améri-

cains avaient mis en place des procédures de transmissions robustes avec des codes redondants très efficaces. On constata une fois encore la mauvaise fois des Anglo-Saxons, qui attribuèrent ce défaut à Myosotis, alors qu'elle n'y était pour rien !

Puis eut lieu la préparation de la mission à Washington auprès de l'agence d'évaluation du Comité Militaire de l'Alliance (SECAN). C'est ce laboratoire qui doit procéder à l'évaluation cryptologique du matériel et proposer au Comité Militaire son approbation pour la protection des informations classifiées de l'OTAN[6].

À Washington, l'équipe est installée dans un bâtiment de l'Ambassade de France. Son mentor est le Capitaine de Vaisseau Henri Lavollay, membre de l'équipe de l'Attaché Militaire près l'Ambassade de France. Il fera tout son possible pour faciliter la mission confiée à MM. Dumaire et Corréard. Le matériel est présenté aux agents du SECAN qui se familiarisent avec son fonctionnement. Toute la documentation, rédigée en anglais, leur est communiquée ; cela dure une quinzaine de jours, au terme desquels, le matériel est transféré au SECAN qui prend en main tous les équipements sans que l'équipe française puisse intervenir. En particulier, l'étude mathématique et statistique, leur fut aussi intégralement transmise. Mais le SECAN ne fit aucun commentaire à ce sujet, comme d'ailleurs pour les autres éléments de son évaluation.

Parmi les contrôles effectués, outre ceux relatifs à la qualité cryptographique de la machine, les américains ont demandé aux Français de calculer (essentiellement à la main) quelques cryptos de Myosotis, sans leur laisser la possibilité de l'utiliser. Le but de cette demande était de vérifier que son fonctionnement réel était bien conforme à la documentation fournie. C'est Corréard qui opère ce chiffrement manuel. C'est un véritable exploit que réalise là Corréard, car pour effectuer correctement ce calcul, qui représentait un nombre gigantesque d'opérations logiques, il fallait connaître les plus petits détails de la machine, et bien sûr ne jamais se tromper alors que rien n'est plus facile que de confondre les 0 et les 1 !

Corréard met deux semaines pour effectuer ces calculs et finalement, les Américains vérifient que le résultat fourni est bien identique à ce que trouve Myosotis ! M. Corréard restera une quinzaine de jours supplémentaires pour pallier un éventuel problème.

Finalement, l'OTAN choisit la machine anglaise Alvis, laquelle était la plus chère et sans doute la moins bonne !

Mais, environ 6 mois plus tard, le STCCh informera la CSF du résultat de l'évaluation par SECAN : Myosotis obtient l'approbation du Comité Militaire pour la pro-

6. Selon les règles de l'OTAN, pour chiffrer du secret OTAN avec un procédé national, celui-ci doit avoir obtenu l'aval du Comité Militaire, donc du SECAN.

tection des informations de toutes classifications OTAN. La machine Myosotis est donc approuvée OTAN. C'est un beau succès[7] !

Pour la petite histoire, André Muller apprendra plus tard que les Américains avaient trouvé que Myosotis était en fait la meilleure machine ; mais d'autres considérations avaient prévalu !

3.7 Le concours interne français et la décision du Ministre de la Défense

Simultanément, se déroulait le concours interne français qui visait aussi à choisir une machine pour la France. Comme nous l'avons vu, au début trois projets étaient en concurrence : la machine Myosotis de l'Armée de Terre, la machine Violette de l'Armée de l'Air, et la machine Ulysse de la Marine.

Le STTA avait supporté financièrement la SAGEM pour étudier Violette. Cette machine était caractérisée par sa compatibilité avec la KL-7 et ses permutateurs Sillet. Ces permutateurs permettaient de découper les alphabets en deux parties et, par composition, de créer des alphabets « aléatoires ». En fait Violette avait deux modes de fonctionnement. L'un était une émulation de la KL-7, l'autre était plus compliqué. La théorie était inspirée des idées de M. Suchard qui enseignait les probabilités et l'informatique à l'Université de Paris. Mais la logique de Violette étant proche de l'esprit « rotor », elle était mal placée pour le concours OTAN qui précisait « *rotorless* ». En outre, elle utilisait des thyratrons à cathode froide, qui se sont révélés être un sérieux handicap : manque de fiabilité et de discrétion (problème TEMPEST), poids et volume très importants, etc.

Quant à la Marine, elle prétendait qu'elle était sur le point de présenter un prototype, mais la machine Ulysse rencontrait quelques difficultés techniques (sa mémoire était constituée de condensateurs) et seuls quelques exemplaires furent construits.

Pour des questions de prix, lequel évidemment dépend évidemment des quantités à produire, l'ÉMA prend la décision de désigner une seule machine de cryptographie pour toutes les administrations. Sa décision s'appuiera sur l'avis technique du STCCh et, au point de vue financier, sur le prix auquel pourra être vendue une telle machine. Ce choix était aussi conditionné par l'obtention de l'approbation OTAN.

L'équipe d'évaluation du STCCh était pilotée par Llopis, secondé par Michel Silvestre et Jean-Paul Fabreguettes, ainsi que le commandant Christian Fabre. En 1962, les lieutenants André Cattieuw et Georges André, détachés de l'armée de l'Air,

7. Mais il faut avouer que ce fut une victoire à la Pyrrhus : la France devait sortir de l'Organisation Militaire du Traité de l'Atlantique Nord en mars 1966, de sorte que la CSF n'eut guère l'occasion de fournir des matériels de chiffrement aux Armées de l'OTAN. Et les services américains étaient en possession de tous les détails de Myosotis !

les rejoindront dans le cadre du projet Violette, tandis que Fabre devenait l'adjoint du bureau Chiffre de la base aérienne 134. En outre, comme indiqué au paragraphe 4.3, elle disposait de nombreux conseillers scientifiques.

Rapidement, André Cattieuw se révéla éminent cryptologue. Sa collaboration au STCCh dépassa les limites strictes du projet Violette et fut aussi chargé de l'évaluation de Myosotis. Il resta au STCCh, où il devint très tôt l'adjoint de Muller, et lui succéda à la tête du service en 1976.

Cette équipe travaille essentiellement sur des données théoriques : elle effectue une évaluation papier, à partir des données des constructeurs. Ces calculs concernent principalement le fonctionnement des registres, les périodes des machines, les probabilités de recouvrement,... André vérifie que Violette est compatible avec la KL-7 et que sa version nationale est supérieure à la KL-7 (sa période est plus grande). Mais il trouve que la période de Myosotis est supérieure à celle de Violette. De son côté, Llopis démontre que Ulysse présente des faiblesses théoriques : elle engendre des groupes (au sens mathématique du terme). Sa sécurité est donc jugée insuffisante par la Sous-Commission Cryptologie. Dans ces conditions et devant les difficultés techniques rencontrées, cette dernière se retire assez vite de la compétition ; le choix ne réside plus qu'entre Myosotis et Violette.

Pour comparer le prix des machines, le SCTI envoie aux deux sociétés concernées, CSF et SAGEM, une demande de prix pour une centaine de machines.

En fait, tant que l'industrialisation n'est pas faite, il est très difficile de fixer un prix. Pour la CSF, Ameil fait le raisonnement suivant. Pour un matériel fabriqué en très grande quantité (téléviseurs, par exemple) le prix des matières premières peut représenter un pourcentage allant jusqu'à 80% du prix de revient, mais pour une quantité n'exigeant pas des frais d'industrialisation importants, la part des matières premières se situe entre 30 et 50%. Ne voulant pas interroger Levallois directement, il était difficile à Xavier Ameil de donner une évaluation pertinente, mais il lui fallait répondre.... Il obtint par l'équipe technique les éléments essentiels qui lui permirent de connaître, à peu près, le prix des matières premières. Puis il doubla à peu près ce prix pour obtenir le prix de revient, d'où le prix de vente, en tenant compte de la marge habituelle dans l'industrie des Télécommunications. Pour être sûr de gagner la compétition financière, il alla voir l'ingénieur général Casal qui lui fit comprendre que le prix envisagé était valable pour éliminer le concurrent, c'est à dire la SAGEM, au point de vue financier.

Restait à être aussi le premier au point de vue technique.

André Muller et André Cattieuw avaient examiné de près Violette. Ils avaient un bon dialogue avec la SAGEM. Il fallait donc les convaincre de faire un examen des études de Gaubert et de Vasseur. M. Muller s'est montré attentif au nouveau « bébé » et a pris conscience de l'intérêt du projet CSF. Un climat de très bonnes relations s'instaura. Le tout premier projet que Vasseur soumit à la sous-commission Cryptologie

fut jugé insuffisant : la période était trop courte. Vasseur présenta un second projet dont la période était cette fois suffisante. La mise à la clé qui consistait à enficher des permutateurs sur des connecteurs particuliers, était séduisante car elle offrait un très grand nombre de clés possibles ; mais le STCCh fit remarquer que tous les permutateurs n'avaient pas le même effet sur le calcul du crypto : la logique de Myosotis présentait une légère dissymétrie due à sa structure en couches successives, dont cependant l'avantage était de masquer vis-à-vis de la sortie les éléments les plus secrets. Mais Vasseur trouva le remède à ce défaut : il proposa d'introduire un re-bouclage dans la logique de Myosotis, re-bouclage qui rendait symétrique le rôle des permutateurs. Finalement ce schéma fut adopté et ce fut la version finale de Myosotis. Petit à petit, Muller fut convaincu de la supériorité technique de Myosotis et il décida de soutenir ce projet.

Par ailleurs, pour l'aspect opérationnel, il fallait également convaincre les utilisateurs futurs du produit, représentés essentiellement par le Bureau Chiffre, tenu d'abord par le Colonel Cullmann puis par le Colonel Samson. Ils furent assez vite convaincus par Myosotis. Ils considéraient que les conditions d'exploitation de la machine étaient très sensiblement plus simples que celles de Violette, mais aussi que sa taille et son poids permettaient d'envisager un matériel tactique nécessaire à l'Armée de Terre. *A contrario*, Violette était un matériel d'infrastructure dont le poids et l'encombrement permettaient son emploi sur les bases aériennes mais certainement pas à bord de « *shelters* » ou de véhicules militaires. Tous ces éléments ont participé à la prise de position en faveur de Myosotis.

Cependant sur le plan technique le choix restait difficile. La difficulté résultait d'une querelle d'experts au sein de la Sous-Commission Cryptologie de la Commission Interministérielle des Chiffres, entre les tenants de Violette et les partisans de Myosotis. Querelle de cryptologues d'autant plus redoutable qu'on ne sait pas démontrer la valeur cryptologique d'un procédé de chiffrement ...sinon en montrant qu'on sait le décrypter ! et donc qu'il n'est pas bon ! Or, les sommités universitaires consultées, dont M. Le professeur Fortet, pour arbitrer le débat se montraient fort prudentes devant l'enfer de complexité présenté par l'une et l'autre machine.

En plus de l'étude théorique et mathématique, la CSF avait produit une étude statistique très riche, ce qui n'avait jamais été fait à cette échelle, dans le monde des cryptologues français. La Sous-Commission était embarrassée pour donner un avis sur ce document. Ce dernier a été évalué finalement par le principal conseiller scientifique du STTCh, le professeur Barra.

Cette étude statistique a pesé dans le choix final de Myosotis. Mais le débat aura été tranché en prenant aussi en considération les aspects afférant à l'emploi : Violette, compatible avec la KL-7 dans un de ses modes de fonctionnement, apparaissait séduisante car pouvant s'insérer petit à petit dans les réseaux de chiffrement existants, tant nationaux que OTAN, mais la technologie utilisée conduisait à un maté-

riel lourd et encombrant qui convenait uniquement à des liaisons d'infrastructure. Elle ne pouvait convenir aux liaisons tactiques de l'Armée de Terre qui avait besoin d'un produit plus léger comme Myosotis.

Dans ces conditions, l'ÉMA décida que Myosotis serait la machine officielle dont devaient être équipées pour la cryptographie les trois Armées. Les autres Administrations, dont le Ministère des Affaires Etrangères, suivirent l'avis de la Sous-Commission et firent le même choix : Myosotis restait la seule machine à chiffrer pour la France.

Par ailleurs, le bloc de chiffrement, contenant toute la logique de Myosotis, fut classé « Diffusion Restreinte » et son bloc de commande, qui contenait ses fonctions d'exploitation, ne fut pas classifié.

La décision officielle fut prise par le Ministre de la Défense, M. Pierre Messmer, en 1965.

Le gouvernement décida de récompenser les principaux acteurs de « l'opération Myosotis » : André Muller remit les insignes de chevalier de la Légion d'Honneur à Jean-Pierre Vasseur en 1968 et à Xavier Ameil en 1971.

4 La fabrication de Myosotis et la création de l'industrie du chiffre en France

4.1 Le développement industriel de Myosotis

L'aboutissement du projet Myosotis marquait une avance de la Thomson-CSF dans le domaine du Chiffre, non seulement sur le plan national mais aussi au plan international.

Mais à la suite du choix de Myosotis, SAGEM avait demandé une compensation. Dans le cadre d'un protocole d'accord, suscité par le SCTI, il est décidé que SAGEM participera à la fabrication en série des Myosotis : SAGEM fabriquera le sous-ensemble de commande télégraphique, CSF se réservant le bloc chiffrant.

En réalité, cette décision avait été anticipée par un compromis négocié par Roger Aubert, Directeur Technique Général de la CSF, et son homologue de la SAGEM. Par cet accord, Aubert s'assurait que la machine Myosotis serait choisie et SAGEM, en acceptant ce choix, obtenait une fabrication de matériels et surtout conservait une place dans le domaine de la cryptographie. En fait, la SAGEM détenait le marché des claviers perforateurs-chiffrants (pour le Ministère de l'Intérieur) et celui des TAREC (pour les Armées et le Ministère des Affaires Etrangères). Mais cela ne lui donnait guère de savoir-faire en matière de machine à chiffrer, d'autant qu'elle ne faisait rien, malgré les sollicitations du STCCh, concernant la production des bandes-clés associées aux TAREC, production qu'il fallait améliorer et moderniser !

Sur le long terme, ce calcul s'est révélé payant pour la SAGEM. En effet, même si la CSF restait la première pour la conception des matériels cryptographiques, la SAGEM réussit à s'introduire dans ce domaine en jouant la carte de la complémentarité, principalement autour de produits qui lui étaient propres (téléphones, téléimprimeurs...). Petit à petit, elle a renforcé son équipe de recherches en scientifiques et cryptologues (souvent avec l'aide du STCCh et même de la CSF, entre autre par le biais des cours de cryptologie que le STCCh organisait et auxquels contribuaient les spécialistes de la CSF !). Et la SAGEM est ainsi devenue le second fournisseur de matériels de chiffrement pour les administrations françaises.

Sans doute parce qu'il pressentait cela, Vasseur ne fut pas du tout content de cet accord ! En effet, il pensait qu'il serait très difficile de faire vivre en France deux fabricants de matériels de chiffrement. Mais cette situation était, somme toute, plutôt confortable pour les administrations françaises qui pouvaient faire jouer la concurrence. Heureusement, une sorte de modus vivendi s'établit de fait entre les deux sociétés et la concurrence ne fut pas trop pernicieuse.

Il fallait maintenant organiser la fabrication industrielle des Myosotis. Il était évident que le laboratoire de RPC devait se retirer de cette affaire et qu'il fallait confier sa fabrication à une unité de la division Matériels.

M. Dumaire quitte alors RPC en septembre 1966 pour transférer le laboratoire Chiffre sur le centre de Levallois où il regroupe l'équipe de Seignol et Samain. Il ne reste à Puteaux qu'une petite équipe, sous la direction de Vasseur, pour le prolongement des études de base, principalement mathématiques et informatiques, nécessaires à l'évolution des matériels, des composants et des besoins exprimés par les armées et les administrations. D'ailleurs ces nouveaux besoins, suscités par les possibilités grandissantes de l'électronique devaient entraîner un flux d'études continu sur plusieurs années. Ceci incite rapidement Vasseur à renforcer son équipe et à lancer de nouvelles études. C'est ainsi qu'il recrute, en janvier 1967, Gilles Ruggiu (venant du STCCh) qui mettra la dernière main aux rapports techniques de Myosotis et participera à la conception et à l'évaluation des machines qui vont succéder à Myosotis.

Pour la CSF, Vasseur reste l'interlocuteur privilégié auprès des instances gouvernementales pour tout ce qui concerne le Chiffre.

Enfin la fabrication de Myosotis est confiée au centre de Cholet, rattaché à Levallois depuis sa création en 1936. L'usine de Cholet commence l'industrialisation de Myosotis en 1964 et sa fabrication en série en 1966. Elle était dotée d'un service d'étude et de développement. Une section de ce service prend en charge ce nouveau matériel avec MM. Candelier et Lamotte qui avaient participé à l'étude et à la réalisation des prototypes à Puteaux et à Levallois.

Au début de la conception de Myosotis, les transistors au silicium ayant des performances suffisantes n'étaient pas disponibles. C'est pourquoi les transistors au

germanium avaient été choisis. Mais à l'époque du lancement de la fabrication des Myosotis à Cholet, les transistors au germanium commençaient à être supplantés par les transistors au silicium. Cependant l'usine de Cholet ne put prendre en compte cette évolution technologique : les délais de fabrication étaient trop courts et la reprise de la conception des Myosotis dans cette nouvelle technologie juste au moment de l'industrialisation aurait été trop coûteuse. C'est pourquoi la filière germanium fut maintenue pendant plusieurs années par l'usine de Saint-Egrève.

À titre indicatif voici les caractéristiques physiques de cette version de Myosotis, avec les protections électriques et radioélectriques (fusibles, filtres) :

f

Ensembles	Largeur (mm)	Hauteur (mm)	Profondeur (mm)	Poids (kg)
Bloc de chiffrement	455	340	370	48
Bloc de commande	200	390	420	19

Sa fréquence d'horloge était de 1 Mhz.

Ce n'est que plus de vingt ans plus tard qu'une version au silicium (en circuit intégré à grande échelle : VLSI), beaucoup plus compacte et légère, fut fabriquée, sur une commande du Ministère des Affaires Étrangères.

Le développement de Myosotis fut une véritable révolution pour Cholet et Levallois. C'était à la fois la première réalisation d'un système numérique, le premier matériel à transistors et l'équipement le plus complexe jamais réalisé à Cholet. La machine comprenait environ 1000 transistors et 4000 diodes. Avant d'insérer les composants, il fallait percer 18000 trous dans les cartes de circuits imprimés. Le problème du test final était aussi difficile à résoudre, pour une machine destinée à produire des caractères aléatoires. L'équipe de Cholet sut très bien résoudre tous ces problèmes. Les machines produites se sont avérées d'une grande fiabilité et les coûts de productions ont été bien maîtrisés puisque les prix de vente laissaient une marge confortable.

En 1968, à la suite de la fusion de la CSF et de la Compagnie Française Thomson-Houston-Hotchkiss-Brandt (CFTH-HB) pour constituer la Thomson-CSF, le laboratoire de Levallois fut transféré sur le centre de Gennevilliers, l'usine de Cholet lui étant rattachée. En 1969, l'équipe de J.-P. Vasseur s'installa à Corbeville, au Laboratoire Central de Recherches de la Thomson-CSF.

4.2 La fourniture des myosotis et le problème de son exportation

En 1974, mille machines auront été réalisées par Cholet et, au total, ce sont mille cinq cents équipements qui sortiront de l'usine de Cholet. Signalons que, grâce à

l'habilitation OTAN, un ensemble de deux équipements (un pour chaque extrémité de la ligne) ont même été fournis à la Norvège pour protéger une de ses liaisons !

Les trois Armées et le Ministère des Affaires Etrangères se sont équipées de Myosotis.

L'Armée de Terre, imitée par les Affaires Etrangères, privilégie le chiffrement en ligne au sein de ses centres de transmissions et ses chiffreurs deviennent des crypto-télégraphistes. Par contre, l'Armée de l'Air, son souci d'économie rejoignant son souci de sécurité, fait exploiter ses Myosotis hors ligne par des sous-officiers régulateurs chiffreurs.

Mais il faut noter que les marins et les aviateurs s'équipent aussi de matériels américains, dont la KW-7 et la KW-37 ! Cette dernière est une machine à chiffrer en ligne pour téléimprimeurs électroniques avec une vitesse maximale de 75 bits/s. Elle est d'un niveau de sécurité nettement inférieur à celui de la KW-7 (sa période, d'environ $5,4.10^9$5,4.109, est cependant correcte), mais elle possède une fonction supplémentaire qui rend plus souple son utilisation : un mécanisme de rattrapage à 25.000 bits par seconde permet d'établir des transmissions en léger différé.

Caractéristique de cette évolution et de l'interpénétration du Chiffre et des Transmissions, provoquée par l'automatisation des opérations de chiffrement, l'Instruction Interministérielle 500/STCCh du 23 décembre 1968 officialise pour l'Administration, à côté des centres ou ateliers de chiffrement qui subsistent, l'existence de centres de transmissions protégés. Elle officialise aussi les méthodes de chiffrement en circuit ainsi que le chiffrement de voie continu ou discontinu qui constituent un progrès considérable par rapport aux errements antérieurs. Les retards imputés au chiffrement disparaissent au prix, certes, d'un investissement en matériels de chiffrement de coût élevé : une machine Myosotis avec son modem filaire coûtait 250 000 F. en 1970.

Les Ingénieurs d'Armement et, en particulier, ceux de la SEFT et du SCTI, ont, tous, contribué au bon développement du Chiffre en France. Conscients de l'importance de l'enjeu que représente le matériel « Chiffre », leur préoccupation majeure était d'assurer aux Armées et aux autorités gouvernementales le meilleur Chiffre possible. Tout en sachant prendre en compte les contraintes économiques, ils n'ont jamais sacrifié la technique. Ils ont su faire confiance aux industriels et ont su leur éviter bien des difficultés, même si la tentation était forte de faire jouer la concurrence entre SAGEM et Thomson-CSF. Il faut souligner l'action efficace du Commandant Tariel en faveur du développement industriel de Myosotis et des nouvelles applications (comme le fac-similé) qui ont immédiatement suivi son déploiement.

La grande question fut la fourniture de Myosotis aux pays étrangers qui n'étaient pas membres de l'OTAN. Ce marché intéressait évidemment la Thomson-CSF. Malheureusement, la France n'avait pas de politique d'exportation pour ce type de matériel, ni de crédits pour proposer une machine dérivée de Myosotis et adaptée aux

besoins de ces pays. En effet, il était clair qu'on ne pouvait la vendre telle quelle. Le STTCh avait demandé à la Thomson-CSF d'étudier une version de Myosotis pour l'exportation, mais celle-ci est restée dans les « cartons », faute de soutien politique et financier.

En fait, parler de la machine Myosotis ou la montrer à des personnalités de pays étrangers, à l'occasion de leur visite, amenait inéluctablement de la part de ces personnalités la question de l'exportation de ce matériel. Or, par ignorance des questions de sécurité nationale, les autorités françaises, au plus haut niveau, déclaraient souvent qu'il n'y avait pas de problème ; autrement dit, elles laissaient entendre que l'on pouvait leur en fournir. Mais ensuite, tout le monde était très ennuyé quand le pays faisait une demande d'achat de machines Myosotis, et personne ne savait comment répondre à cette demande.

Devant cette situation et par manque de politique d'exportation, le STCCh a demandé de cacher l'existence de Myosotis ! Les chiffreurs reçurent l'ordre de n'en pas parler et de considérer le nom même de Myosotis comme classifié.

Cet état de chose a, d'ailleurs, conduit à introduire les moyens de cryptologie dans le décret de 1973 régissant les matériels de guerre, et le STCCh à prôner une politique officielle d'exportation. Mais se posait alors le problème du financement des études du matériel destiné à l'exportation, financement que la Thomson-CSF ne pouvait supporter toute seule. Malgré les exhortations de STCCh, l'État-Major, qui détenait les crédits militaires pour le matériel « Chiffre », soutenait que ce n'était pas son problème, son objectif étant d'équiper les forces ; et la Défense, de son côté déclarait qu'elle mettrait son veto à toute demande d'exportation hors OTAN. Ce problème ne fut pas résolu et, plus tard, la même question s'est posée, sous une autre forme, avec le chiffre civil.

4.3 Les conséquences scientifiques et industrielles du projet Myosotis

La machine Myosotis a été conçue et étudiée par la CSF, mais en collaboration avec la DMA (devenue plus tard la DGA), le STCCh (aujourd'hui la DCSSI, Direction Centrale de la Sécurité des Systèmes d'Information, rattachée au Secrétariat Général de la Défense Nationale) et la Sous- Commission « Cryptologie » de la CIC.

Le succès du projet Myosotis est dû à l'excellente coopération des administrations, des industriels et des nombreux scientifiques qui ont assisté soit le STCCh, soit la CSF. Ces bons rapports n'empêchaient pas d'âpres discussions entre les différents spécialistes, discussions d'autant plus délicates que peu d'arguments étaient susceptibles d'être prouvés !

Outre ses propres experts et ceux de la Sous-Commission Cryptologie, le STCCh avait de nombreux conseillers scientifiques, le plus souvent bénévoles. Les principaux d'entre eux furent : J. Favard, professeur à la faculté des sciences de Paris et

à l'École Polytechnique ; Paul Dubreil, professeur d'algèbre à l'Université de Paris ; le professeur Dugué, directeur de l'Institut Supérieur de Statistique de l'Université de Paris, ainsi que le Colonel Georges Cullmann, ancien patron du bureau Chiffre de l'Armée de Terre, conseiller scientifique de la compagnie des machines Bull et professeur à l'École Supérieure d'Électricité. Mais pour l'étude de Myosotis, le principal collaborateur scientifique du STCCh fut J. R. Barra, professeur de Statistique à l'Université de Grenoble. Il établit les fondements de l'évaluation statistique des machines à chiffrer.

Le principal collaborateur scientifique de la CSF fut André Berroir, professeur de mathématiques à l'Université de Paris. Il contribua à la théorie du fonctionnement de Myosotis. En concertation avec Barra, il proposa beaucoup de tests dont il mit au point les lois théoriques. Il savait aussi tenir compte des aspects pratiques et concrets : c'est lui qui fixa les règles d'interprétation des résultats expérimentaux, interprétation très délicate eu égard à leur nombre.

Il faut aussi citer Pierre Aigrain qui marqua beaucoup d'intérêt pour ces travaux et pour le Chiffre en particulier.

C'est le grand mérite d'André Muller, et aussi de Jean-Pierre Vasseur, d'avoir su faire travailler ensemble toutes ces individualités, en bonne intelligence et estime réciproque. J.-P. Vasseur était invité régulièrement par A. Muller aux réunions de la Sous-Commission pour en recevoir les critiques et discuter des solutions.

Le projet Myosotis a permis de fixer la doctrine française de conception et d'évaluation des machines à chiffrer. Ce sont les travaux d'analyse et d'évaluation de Myosotis qui ont donné une base scientifique à cette doctrine. En effet, c'est en s'appuyant sur les travaux de Shannon et sur l'expérience des cryptologues et des chiffreurs, qu'ont été fixées les bases du savoir-faire en matière de conception algorithmique des machines à chiffrer et de prise en compte des contraintes d'utilisation.

Par ailleurs, sont étudiées et mises en œuvre, sous l'égide du STCCh, les méthodes et procédures d'analyse et d'évaluation des machines à chiffrer, d'une part au plan cryptologique et d'autre part au plan des rayonnements compromettants (TEMPEST).

Ce dernier sujet constituait un domaine nouveau, les mesures correspondantes pour vérifier la conformité aux normes firent l'objet de nombreux examens. Au début aucune norme n'existait en matière de rayonnements compromettants : aucune règle ne précisait les conditions de mesure. Il a fallu s'équiper de matériels spéciaux et très sophistiqués pour dégager des principes. La Thomson-CSF, mais aussi la SAGEM, acquièrent, de fait, une grande compétence dans la mesure, l'analyse et la maîtrise de ces rayonnements compromettants. Elles constituent assez vite un grand savoir-faire tant en ce qui concerne les filtres que les règles de câblage et de blindage. Petit à petit une doctrine en matière d'évaluation et d'instal-

lation des ensembles cryptographiques concernant l'aspect TEMPEST finit par être agréée.

Cette doctrine a été concrétisée par l'Instruction Interministérielle sur les rayonnements compromettants et les règles techniques de sécurité des matériels des communications 300/STCCh du 7 avril 1973.

Si les bases théoriques et scientifiques de la cryptologie (mathématiques, statistiques et algorithmiques) sont bien connues au STCCh, en fait l'application industrielle de toutes ces connaissances et les outils de mise en œuvre sont essentiellement maîtrisés par la Thomson-CSF et l'équipe de Jean-Pierre Vasseur. Celle-ci a, en outre, accès aux derniers développements des technologies électroniques (T2L, MOS, CMOS,...) et sait en tirer le meilleur parti pour optimiser la logique et le fonctionnement des machines à chiffrer. Les nouvelles machines en bénéficieront grandement. On peut dire que seule la Thomson-CSF, en tant que fabricant industriel, est, à cette époque, en mesure de concevoir les nouvelles machines à chiffrer dont la France va avoir besoin.

5 Conclusion

Le projet Myosotis fut la conséquence de la volonté de l'État français de se doter de moyens de chiffrement modernes, sûrs et adaptés à ses besoins. L'importance et la qualité des travaux qui ont abouti à la réalisation de cette machine ont permis de doter la France non seulement d'une doctrine du Chiffre cohérente, mais aussi de structures étatiques et industrielles qui l'ont placée au tout premier rang dans le monde dans le domaine de la cryptographie.

La position de la France s'est ensuite maintenue pendant une trentaine d'années grâce aux développements ultérieurs de nouveaux systèmes cryptographiques, développements dont la vigueur a encore été accentuée par les progrès considérables que l'électronique et les communications ont connus durant cette période. Avec l'introduction progressive de l'informatique dans les divers systèmes d'information, les conditions d'utilisation du Chiffre se sont considérablement modifiées en évoluant vers une intégration dans ces systèmes toujours plus poussée et une automatisation sans cesse accrue.

À partir du début des années quatre-vingt-dix, l'apparition du Chiffre civil et le formidable essor d'Internet ont posé de nouveaux problèmes. Les besoins des civils ainsi que leur façon d'utiliser le Chiffre étaient différents de ceux des gouvernements. De nombreux systèmes de chiffrement, en majorité d'origine américaine, sont alors apparus sur le marché dans une anarchie d'autant plus complète que les nouveaux utilisateurs du secteur civil n'avaient aucune compétence et aucun repère pour se faire une idée de leur valeur.

Les États, qui, comme la France, avaient une politique concernant l'emploi de moyens de cryptologie, avaient besoin de conserver un certain contrôle sur la fabrication et l'utilisation de ces moyens. Ils ont eu beaucoup de mal à réagir pour faire face à cette situation nouvelle d'autant plus que, comme pour tous les systèmes d'armes modernes, les outils développés dans ce domaine pour le civil ont un impact sur le militaire.

Un certain nombre de dispositions ont alors été prises, mais certaines erreurs ont été commises. Aujourd'hui encore, la situation du Chiffre en France, comme dans d'autres pays développés, est confuse et peu satisfaisante, instaurant, à l'opposé du but recherché, un climat de défiance envers la cryptographie et les services étatiques. Nous pouvons donc dire que, lorsque s'est effacée, au début des années quatre-vingt-dix, l'impulsion donnée par le projet Myosotis, une page de l'histoire de la cryptographie en France a été tournée.

Biographie des auteurs

Xavier Ameil : Ingénieur diplômé de l'École Polytechnique et de l'École Nationale Supérieure des Télécommunications. Ancien directeur adjoint du laboratoire de Recherches Physico-chimique de la CSF.

Jean-Pierre Vasseur : Ingénieur diplômé de l'École Centrale de Paris ; Docteur ès-Sciences. Ancien chef de laboratoire au Laboratoire Central de Recherches de la Thomson-CSF, puis Directeur Technique de Thomson-Brandt.

Gilles Ruggiu : Ingénieur diplômé de l'École Nationale Supérieure des Télécommunications ; Docteur ès-Sciences. Ancien chef de laboratoire au Laboratoire Central de Recherches de la Thomson-CSF, puis Directeur de l'informatique de la société Bertin.