De la C-36 à la carte CP8

Jean-Louis Desvignes

Une nouvelle période sombre

Après les exploits de la Grande Guerre, je dois malheureusement parler d'une nouvelle période sombre de la cryptologie française avec la défaite de 1940 avant d'évoquer un véritable rebond dans la seconde partie du XXe siècle.

En effet, nos stratèges victorieux en 1918 étaient certainement heureux de devoir rester discrets sur les avantages que les renseignements d'origine technique et en particulier la cryptologie leur avaient apportés. Mais hélas ! de la discrétion à l'oubli, il n'y avait qu'un pas. Et notre cryptologie commença à décliner.

C-36

B-211

Notre armée s'est en effet satisfaite des machines mécaniques C-36 et électromécaniques B-211 fournies par le Suédois Boris Hagelin. Ces machines, d'assez bonne qualité au demeurant, supportaient plus ou moins la comparaison avec les ENIGMA et étaient même plus faciles à utiliser grâce à leur capacité d'impression. Mais, comme d'autres équipements militaires tels que les postes radio ou, plus importants, les avions et les chars, ils ne furent pas utilisés judicieusement, et firent défaut dans la guerre dynamique imposée par l'ennemi. Alors que les ENIGMA accompagnaient les chars du général Guderian, la majorité des B-211 restaient fixes.

Hans Thilo Schmidt

Dans la grande guerre cryptologique contre ENIGMA, la seule véritable contribution de la France a été pour les services de renseignement, en particulier le colonel Bertrand, d'avoir su gérer la trahison de Hans Thilo Schmidt, le traître allemand que David Kahn a qualifié de plus grand espion de tous les temps. Cette contri-

bution a parfois été minimisée, mais il est difficile de soutenir que la livraison régulière des manuels d'instructions et des tableaux de clés d'ENIGMA n'a pas été un avantage significatif pour sa cryptanalyse.

Le canal de Suez en 1956

À la fin de la guerre, la cryptologie française était à son plus bas. Notre réveil fut brutal quand en 1956 les Britanniques nous révélèrent qu'ils ne pouvaient pas s'embarquer avec nous dans la reconquête du canal de Suez nationalisé par Nasser si nous utilisions les vieilles machines de M. Hagelin qu'ils lisaient ouvertement. Comme les Américains d'ailleurs à qui nous les avions données à évaluer.

C'est alors que le gouvernement Français décida de consentir un effort dans ce domaine par trop négligé.

Un nouveau printemps : Myosotis

La France n'était pas la seule à devoir réinventer sa cryptologie car les équipements hérités de la Seconde Guerre mondiale n'étaient plus adaptés aux moyens de communication modernes. En 1957, un concours fut lancé entre ses trois armées tandis que, dans le même temps, l'OTAN lançait un concours pour renouveler ses machines à rotor américaines KL7.

Myosotis

En France, c'est la machine de l'armée de terre Myosotis, la première machine électronique, qui l'emporta, grâce à ses performances cryptologiques, sa facilité d'utilisation et sa taille limitée, un facteur essentiel pour les forces terrestres. En outre, cette machine passa avec succès le test d'évaluation de l'agence SECAN. Dans la compétition de l'OTAN, face à la KW7 américaine, l'ALVIS britannique et l'Elcrovox allemand, elle ne pouvait gagner pour des raisons politiques. Mais l'approbation par le comité militaire fut un premier succès. Elle équipera toutes les forces françaises et la diplomatie, et se révélera très fiable.

C'est à elle, d'ailleurs, que je dois d'être parmi vous. En effet, jeune lieutenant, mon colonel vint à visiter mon shelter de crypto-télégraphistes juste au moment où notre Myosotis venait de s'éteindre. Désastre ! Je n'y connaissais encore rien mais j'ai quand même réussi à trouver le fusible qui s'était simplement dévissé. Immédiatement, j'ai été promu grand cryptologue par ce colonel qui m'a aussitôt inscrit à un stage d'officier chiffre que j'avais réussi à éviter jusque-là…

Myosotis a traversé plusieurs décennies sans problème, à l'exception de la compromission par rayonnement électromagnétique de son téléimprimeur associé découverte dans notre ambassade de Moscou durant la Guerre froide. Nous ne fûmes pas les seuls à avoir été victimes de ce genre de piège de la part des Soviétiques : lors

d'un passage frontalier digne d'un film d'espionnage, avec la complicité d'une petite vertu et de boissons fortes, le condensateur de l'alimentation du téléimprimeur avait été remplacé par un composant identique contenant en fait un amplificateur des signaux compromettants permettant de collecter à distance le texte clair de nos dépêches diplomatiques… Et cela dura au moins six années de 1977 à 1983.

Maintenant, deux événements qui stimulèrent les télécommunications de l'armée française

Le général de Gaulle

En 1965, le général de Gaulle annonce son intention de retirer la France de l'organisation intégrée de l'OTAN. Conséquence : nos Forces qui s'appuyaient, pour leurs télécommunications, sur celles de l'OTAN principalement établies avec des équipements américains, allaient rapidement devoir se débrouiller seules. Heureusement existait dans les cartons un projet de nouveau réseau tactique.

De plus, trois ans plus tard, les manifestations de 1968 qui conduisirent à la grève générale révélèrent la vulnérabilité des communications gouvernementales. Le général de Boissieu, gendre du général de Gaulle, a raconté dans un livre comment il s'est trouvé dans l'impossibilité d'appeler le commandant des forces françaises en Allemagne pour l'avertir de l'arrivée en hélicoptère de son beau-père, les « demoiselles du téléphone » lui refusant de passer la communication. Peu de temps après ces événements, il tomba une pluie d'or sur l'arme des Transmissions afin que celles-ci réalisent un réseau stratégique capable de résister à une guerre mais aussi à ce genre de situation insurrectionnelle : ce fut le RITTER. Quelques années plus tard, le besoin en transmission de données conduisit à la réalisation d'un nouveau réseau sécurisé à commutation de paquets : RETINAT.

Mais tout d'abord c'est le réseau tactique dont les études avaient déjà commencé qui fit l'objet des plus grands efforts.

Manifestations et grève générale en mai 1968

Un grand succès : le réseau tactique RITA

Raccordement RITA d'un PC de Brigade

Notre pays disposait alors d'une recherche publique et privée de pointe. À partir du milieu des années soixante, de nouvelles techniques de communication apparaissent : numérisation, modulation par impulsions codées, commutation électronique, multiplexage, etc. Dans le même temps, au niveau doctrinal, la possibilité émerge de remplacer les réseaux hiérarchiques par des réseaux nodaux (ou zonaux) offrant une plus grande résilience. C'est ainsi qu'émergera un réseau révolutionnaire, RITA : à l'époque, ce fut le premier réseau numérique, à intégration de services (téléphonie, télégraphie, fax, et bientôt données) sécurisé par chiffrement d'artère et permettant la connexion des abonnés mobiles par radio chiffrée.

RITA : combiné

Bref, un réseau GSM avec 20 ans d'avance. D'accord, le téléphone ne tenait pas encore dans une poche de veston, mais ce système plaçait la France en tête de tous les pays occidentaux. À tel point que, renonçant à son propre projet, l'armée américaine l'adopta pour réaliser son réseau MSE. Ronald Reagan lui-même trancha en sa faveur malgré les supplications de Margaret Thatcher qui rêvait de lui faire acheter Ptarmigan, le concurrent britannique.

Je n'ai guère participé au succès de RITA si ce n'est en démontrant sa facilité d'utilisation. Lorsqu'il fut attribué aux forces françaises basées en Allemagne (FFA), le général COMTRANS me demanda d'en effectuer la recette et de donner mon avis. C'est alors que me vint l'idée absurde de faire effectuer cette recette par une troupe de 50 réservistes chevelus dont la formation remontait à plusieurs années et à qui nous ne confiions habituellement que du matériel obsolète… On me traita de fou bien sûr mais bingo ! Ce fut un grand succès. Avant la fin de la journée, je rendais compte à mon général que toutes les liaisons avaient été établies avec une facilité déconcertante et que j'allais renvoyer chez eux des réservistes enthousiastes prêts à affronter le Pacte de Varsovie dans d'excellentes conditions… Ensuite, nous reçûmes régulièrement des visites d'autorités étrangères qui découvraient que ce système moderne, de surcroît, exploitait déjà la numérisation du terrain.

RITA : poste radio PRA

Cela dit, ce système n'était pas sans défaut. Tout d'abord, il avait été bâti avec des composants spécifiques, donc très coûteux. Pour être des pionniers, nous avions parié sur des normes et nous nous sommes trompés. Ex : les PTT choisirent un échantillonnage numérique à 64 kbit/s, et nous 48. En conséquence, les terminaux RITA étaient spécifiques à une époque où les mêmes équipements commerciaux voyaient leur coût chuter drastiquement.

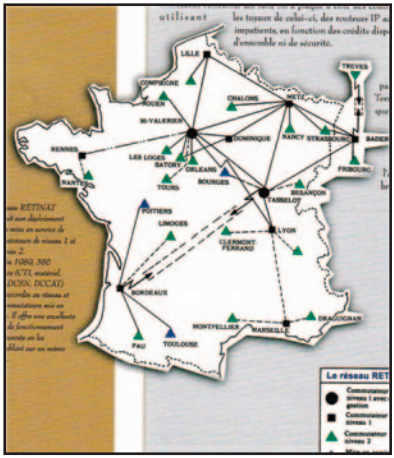
Mais surtout, d'un point de vue sécuritaire, RITA avait été conçu comme une forteresse, un réseau fermé censé être plus facile à protéger. Mais quand il fallait communiquer avec le monde extérieur, via une passerelle manuelle, c'était forcément risqué. Ce fut une leçon pour moi.

Cependant, on dit que cette facilité imprudente fut un facteur déterminant dans le choix américain : le général qui était venu tester le système dans une grande forêt de l'est de la France, eut besoin de contacter le Pentagone. « Pas de problème mon général » et on lui établit immédiatement sa communication « fort et clair » Ce fut l'extase…

Le réseau stratégique RETINAT

Louis Pouzin

En 1979, je fus désigné chef de projet du RÉseau de Transport des Informations Numériques de l'Armée de Terre : RETINAT. Pour commencer, une question difficile : quel type de réseau choisir ? À l'époque, le succès de RITA conduisait ses partisans à ne jurer que par la commutation de circuits. Il fut déjà difficile d'expliquer que la meilleure solution résidait maintenant dans la commutation de paquets mais une fois cela accepté, une autre question terrible : « Circuit virtuel de type X25 » favorisé par les PTT ou « Datagramme » inventé par notre compatriote Louis Pouzin ? Ce dernier type, adopté par l'ARPANET avait de quoi séduire les militaires : il était réputé pouvoir résister à la destruction nucléaire d'un ou plusieurs nœuds… Cependant, les échos qui nous revenaient sur le modèle existant n'étaient pas rassurants : la qualité de service et la fiabilité de l'acheminement, même par temps calme, laissaient à désirer. Le taux d'erreur semblait prohibitif pour un réseau transportant des informations chiffrées. La sacro-sainte exigence d'intégrité binaire ne semblait pas atteinte.



Le réseau initial RETINAT

En revanche, le réseau public TRANSPAC largement déployé à l'échelle internationale mettait en œuvre des mécanismes exigeants pour atteindre un taux d'erreur de 10 -9. C'était un atout décisif à une époque où la faible puissance des machines des utilisateurs ne leur permettait pas de compenser les imperfections du réseau. Il valait mieux pour moi commencer par assurer le parfait fonctionnement de celui-ci en temps normal que de réussir à le faire survivre au milieu d'un pays vitrifié.

Je choisis donc le protocole X.25, en me promettant de respecter au mieux la norme afin d'utiliser un maximum de composants standards et même d'équipements sur étagère.

Commutateur RETINAT

Pour garantir la sécurité du réseau contre les actes malveillants de piratage, toute sa gestion était protégée par le chiffrement des échanges entre les commutateurs et le centre de gestion grâce à un module crypto greffé directement sur la carte mère des commutateurs.

La sécurité des supports était assurée par la redondance et la variété de ceux-ci.

La sécurité des échanges entre abonnés fut confiée à l'équipement crypto Capucine X.25 que je vais vous présenter.

RETINAT a été réalisé dans les délais et les limites du budget prévus et n'a connu aucun incident d'exploitation. Il est resté opérationnel pendant une vingtaine d'années et, le moment venu, a facilité à la fin du siècle dernier, le passage inévitable au protocole INTERNET et à un Intranet de la Défense.

J'ajoute qu'en 1991 commandant alors le 8e RT, j'ai eu le plaisir de recevoir une délégation de l'OTAN au Mont Valérien pour lui présenter ce réseau. Parmi les délégués se trouvaient de nombreux anciens collègues de l'ACCSA dont j'avais rebattu les oreilles des mérites du génie français…

CAPUCINE

Capucine

Lorsque les réseaux à commutation de paquets sont entrés à l'ordre du jour de l'ACCSA, peu de spécialistes en cryptologie savaient de quoi nous parlions. Je me souviens avoir utilisé de petits dessins humoristiques pour expliquer le principe des chiffreurs de paquets :

À l'entrée, un flux de données est injecté sous forme de paquets découpés selon le protocole. Ces données sont désempaquetées puis chiffrées, reconditionnées et enfin réinjectées dans le réseau, les données de routage ayant été conservées. Bien sûr, la réalisation est assez complexe.

Respectant la norme internationale, l'équipement pouvait être utilisé sur tous les réseaux X.25 nationaux et étrangers. Cette normalisation facilita en outre le déploiement du réseau militaire, la transition d'un média à l'autre se faisant sans impact pour l'utilisateur.

Agréé par le SCSSI pour transmettre des informations classifiées SECRET DEFENSE, Capucine a été proposé et approuvé pour protéger les informations de même niveau de l'Union de l'Europe Occidentale (UEO) après une nouvelle évaluation réalisée par l'agence allemande, le BSI. C'était le premier équipement à subir cette double évaluation européenne instituée pour compenser l'absence d'une agence

Chiffreur IP ECHINOPS

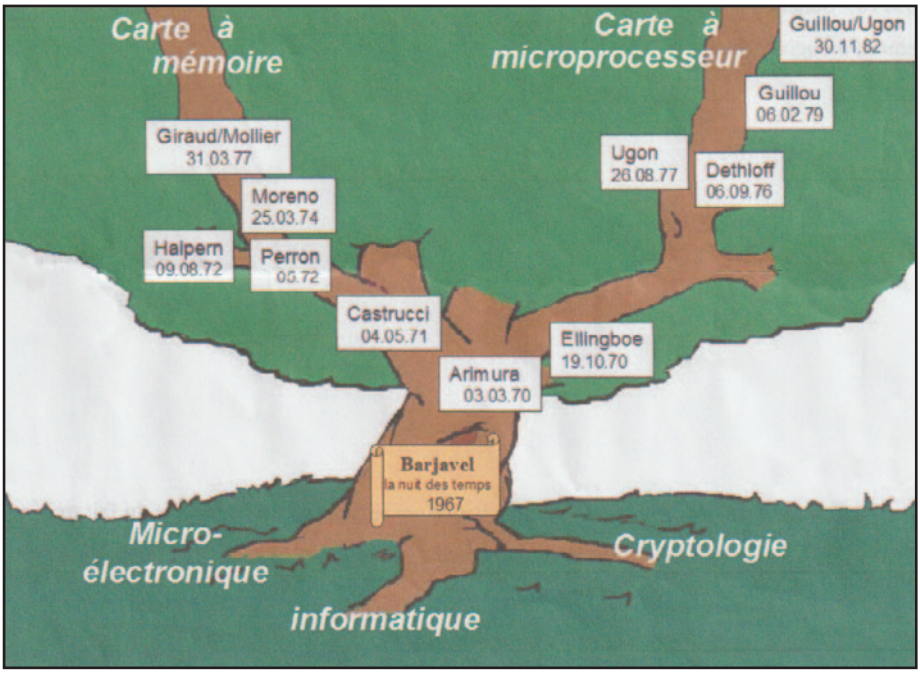
européenne équivalente à SECAN. Le même processus sera appliqué ultérieurement pour le chiffreur IP ECHINOPS de THALES choisi par l'Union européenne. Mais cette fois, il fut réévalué par l'agence britannique, le CESG.

La Carte à puce

Comme nous l'avons vu, l'obligation de voler de nos propres ailes nous a permis de briller en termes de télécommunications militaires sécurisées. Et pas seulement avec les systèmes que j'ai présentés.
Mais ces succès dans le domaine militaire ne sont qu'une petite chose comparée au succès phénoménal rencontré par l'invention du plus petit dispositif cryptographique du moment : la carte à puce.


Michel Ugon

Je ne peux aborder ce sujet sans une certaine émotion car son inventeur Michel Ugon, est décédé en décembre dernier sans que ses mérites aient été reconnus à leur juste valeur.
Seule l'ARCSI lui a rendu hommage immédiatement parce qu'il était l'un des nôtres, et parce que Michel a été victime d'une injustice que nous nous efforçons de corriger chaque fois que nous en avons l'occasion. En effet, un imposteur qui avait sournoisement glané des informations auprès de la société de Michel avait réussi à déposer un brevet pour une simple carte mémoire. Habile communicateur, cet usurpateur a pu bénéficier d'un soutien médiatique qui lui a valu le titre « d'inventeur de la carte à puce ».
Alors que je dirigeais le SCSSI, j'ai personnellement eu l'occasion de mesurer le niveau limité de connaissances de cet imposteur. Avide de publicité, il avait lancé un défi risqué à travers la presse, promettant 1 million de francs à quiconque casserait ses cartes. Puis il a été informé que nous étions capables de le faire en 5 minutes. Il n'avait pas encore entendu parler de DPA (Differential Power Analysis) Vous pouvez imaginer l'état dans lequel il se trouvait lorsque je l'ai remercié d'avoir financé nos prochaines vacances pendant plusieurs années…
Michel Ugon lui, était un brillant ingénieur de la société BULL. Il a en effet été le premier à réussir à installer un véritable processeur sur nos petits morceaux de plastique, ouvrant la voie au développement d'une industrie qui allait inonder la planète. Son premier grand succès a été la carte bancaire CP-8 en 1986. Il est à l'origine de nombreux brevets mais a toujours reconnu ce qu'il devait à ses prédécesseurs (voir arbre des brevets).
Aujourd'hui, des dizaines de milliards de cartes sont utilisées dans le monde dans tous les domaines : cartes SIM, cartes bancaires, cartes de santé, cartes d'identité, etc.



Arbre des brevets de la carte à puce

Modestement, j'avais rapidement identifié l'intérêt de cette technologie pour les équipements cryptographiques militaires afin de sécuriser leur mise à la clef.

Cette solution m'était en effet apparue comme le moyen le plus efficace pour un coût très modeste comparé aux procédés les plus modernes en vigueur (injecteurs de clefs Cry 104). À condition que la carte soit vraiment sécurisée. Heureusement, les critères de sécurité des technologies de l'information étaient en cours d'établissement (TCSEC, ITSEC et enfin Critères communs) et le SCSSI allait choisir la carte à puce comme domaine d'application privilégié de ces critères.

Téléphone TEOREM

Les nouveaux équipements de cryptographie militaires ont donc progressivement intégré cette solution. D'abord utilisées pour des systèmes symétriques classiques, elles sont maintenant utilisées dans les systèmes recourant à une PKI.

Juste une anecdote : en 1986, à l'ordre du jour d'une réunion bilatérale avec la NSA celle-ci avait inscrit la « smart card ». Nous avions donc apporté un exemplaire de notre fleuron du moment, la CP-8. Quelle ne fut pas notre surprise de la voir confrontée à une sorte de calculatrice avec de grandes touches pour personnes âgées. Je ne pense pas que nous ayons été pris au sérieux. Cependant, quelques années plus tard, faisant ma tournée

Signature des accords de reconnaissance mutuelle des certificats délivrés selon les critères communs en 1998

d'adieux à la NSA, ma surprise cette fois fut d'entendre mon collègue américain me demander si le SCSSI pourrait faire bénéficier ses services de son expérience en matière de cartes à puce : le gouvernement américain avait décidé d'en doter tous ses agents. Trop heureux de rendre service à la prestigieuse agence, j'ai répondu positivement. Il était certainement revenu aux oreilles de mon ami que de grandes entreprises asiatiques et même américaines de semi-conducteurs telles que MOTOROLA nous avaient demandé de procéder à la certification de leurs puces.

C'est sans doute ce qui explique pourquoi Barbara McNamara, à l'époque N° 2 de la NSA, en me présentant à son nouveau directeur le général Hayden lui a précisé ; « *Vous savez, le SCSSI est une toute petite agence mais elle fait un sacré boulot !* ».

Aujourd'hui, la carte à puce doit faire face à une évolution en particulier dans l'application la plus utilisée, la carte SIM, qui est maintenant de plus en plus intégrée dans les appareils de communication. On parle de e-SIM. Dans d'autres applications utilisées pour les contrôles d'identité, en particulier les passeports, les cartes de santé, je suis sûr que la carte à puce continuera à prospérer.

C'est sur cet espoir que je termine mon intervention et que je laisse la place à Jean-Jacques Quisquater, spécialiste incontesté non seulement des cartes à puce mais de tout ce qui touche à la cryptologie. Il a été fait membre d'honneur de l'ARCSI il y a une douzaine d'années. Comme il a souvent coopéré avec des chercheurs et des industriels Français, il a spontanément accepté de vous parler des succès les plus récents de la recherche française.

Je vous remercie de votre attention.