Joël Hosatte, Exposé BNF le 26 novembre 2019 :
Les réponses et remèdes apportés par l'Etat jusqu'aux années 2000

Le renouveau du chiffre en France date de la réalisation de la machine MYOSOTIS ; Gilles Ruggiu nous en a compté l'histoire en juillet 2003 dans un bulletin hors-série de l'ARCSI.
Mais voyons d'abord l'organisation étatique en France dans les années 1950.

Les trois armées Terre, Air, Mer sont totalement indépendantes ; chacune est rattachée à un Secrétaire d'État différent et possède sa propre direction pour la réalisation et l'acquisition de ses armements.
A son arrivée au pouvoir en 1958, le Général de Gaulle confirme sa volonté d'acquérir une capacité nucléaire, dont les études avaient commencé dès 1954 en coopération avec les américains. Malgré la présence d'un délégué ministériel pour l'armement auprès du Ministre, les études de missiles menées par les armées sont peu coordonnées.

En 1961, la décision est prise de regrouper les quatre directions en charges de l'armement sous l'autorité directe du délégué ministériel, en y adjoignant une direction de la recherche, et huit départements de coordination, dont un pour les engins –qui deviendra vite une direction- et un pour l'électronique, technologie nouvelle appelée à prendre de l'importance. Le département DEL deviendra le Service central des télécommunications et de l'informatique, dont dépendra le Centre d'électronique de l'armement, créé en 1968 à 12 km de Rennes. Le CELAR est aujourd'hui la DGA/Maitrise de l'information. Le SCTI deviendra la DEI en 1982, coiffant le nouveau Service technique pour les programmes interarmées.
La DMA deviendra Délégation générale en 1977, Direction générale aujourd'hui.

Côté Premier ministre, le 4 janvier 1951 sont créés simultanément la commission interministérielle des chiffres présidée par le Secrétaire général du gouvernement et le Service technique central des chiffres, organe d'étude permanent de la commission. On lui confie en 1958 la responsabilité de réaliser les bandes aléatoires pour les TAREC puis, en 1962, celle du centre de formation créé 2 ans plus tôt au ministère des armées.
L'ANSSI qui vient de fêter ses 10 ans est en fait la digne héritière du STCCh de 1951.

A cette époque, les machines à chiffrer en service dans l'armée française datent d'avant-guerre. Elles sont d'origine suédoise, de la société Boris Hagelin.

Venons-en à la décision de réaliser la machine à chiffrer MYOSOTIS.
Faute de financement pour réaliser le barrage d'Assouan, le président égyptien Nasser nationalise la compagnie du canal de Suez, source de revenus, le 26 juillet 1956. La France et l'Angleterre planifient en secret une intervention militaire en y impliquant Israël. Débutée en octobre, elle s'arrêtera rapidement sous la menace de l'URSS et la pression des Américains.
Le point essentiel qui nous concerne est le refus des Britanniques de nous voir employer nos machines B211, qu'ils peuvent décrypter. Pour mémoire, leur capacité à décrypter Enigma pendant la 2^{e} guerre mondiale ne sera révélée que 17 ans plus tard, en 1973.

Un plan de modernisation est adopté avec l'acquisition de KL7 OTAN et la réalisation de CX 52 sous licence. Mais germe aussi l'idée de réaliser en France une machine électronique. Dispersées comme

elles l'étaient, chaque armée lance son étude et 3 projets de machine voient le jour : - Ulysse pour la Marine ;
- Violette pour l'armée de l'air, étudiée par Sagem et l'armée de l'air, dérivée de la KL7 ;
- Myosotis pour l'armée de terre, étudiée par CSF et la Section d'études et fabrications des télécommunications.

A la même époque, l'OTAN lance un concours pour remplacer les KL7 par une machine électronique, sans rotors. La CSF décide de concourir, malgré les délais très courts de présentation de prototypes en février 63.
Elle est dans les temps et Myosotis franchit avec succès toutes les étapes de l'évaluation OTAN, jusqu'à son approbation par le Comité Militaire pour la protection d'informations de tout niveau de classification.
Mais in fine, l'OTAN choisit d'acquérir la KW7, son concurrent US. Le refus des américains de partager le pouvoir au sein de l'OTAN conduit le Général de Gaulle à retirer notre Marine du commandement militaire intégré en 1962. Le choix d'une machine française devenait alors politiquement incorrect. Pour mémoire, toutes nos troupes sont retirées du commandement militaire intégré en 1966, et notre retour date seulement de 2007.
Myosotis est réalisée en composants discrets, des transistors au germanium ; sa mise à la clé est faite par enfichage d'un jeu de 10 permutateurs, qui seront câblés à la SEFT.

La conception et l'évaluation de Myosotis doivent beaucoup aux travaux que Shannon a effectué sur le chiffre et le codage de l'information au sein des Bell Lab's.
(voir les publications et le stand de Jon Paul sur Sigsaly).
Pour le chiffrement de chaque lettre, Jean-Pierre Vasseur (CSF) et Marius Gaubert (SEFT) imaginent le tirage d'alphabets pseudo-aléatoires.

Le seul système mathématiquement sûr est l'addition du clair avec une clé totalement aléatoire, aussi longue que le message à chiffrer. JP Vasseur recherche l'équiprobabilité des variables internes et le STCCh vérifie que le crypto généré par Myosotis est semblable à de l'aléa vrai. Son chef, M. Müller, sait s'entourer des compétences nécessaires, venant de la Défense et du monde universitaire. Mentionnons le Col Cattieuw de l'armée de l'air, qui deviendra son adjoint puis le Chef de service jusqu'à son passage à la DISSI en 1986 (le Col Cattieuw est un Arcsiste), et le Pr Barra, professeur de statistiques à l'université de Grenoble.
La réalisation de Myosotis fait découvrir le nouveau domaine des signaux parasites qui, si l'on n'y prend garde, peuvent véhiculer et transmettre des informations sensibles.
Réalisé presque artisanalement à l'époque de Myosotis, les tests statistiques seront facilités ultérieurement par la réalisation d'un APpareil de REcueil des DOnnées STATistiques. L'APREDOSTAT a permis de valider notamment la logique Fétiche du RITA, vendu aux américains, et Cryptomod, qui équipe tous les matériels des années 80. Ces deux logiques ont été soumises avec succès à l'évaluation de l'OTAN (SECAN, en fait la NSA).

Une seule machine, MYOSOTIS, est finalement choisie pour équiper les armées et les ministères civils. A titre de compensation, Sagem participe à sa fabrication en série.
Ce sont donc des années 60 que date la capacité française à réaliser des matériels de chiffrement dans lesquels avoir confiance. Les logiques de chiffrement sont conçues par Thomson-Csf jusqu'aux années 90, puis par l'administration.

Les doctrines de conception et d'emploi des machines font l'objet de l'instruction interministérielle 500, qui officialise l'intégration du chiffre et des transmissions, et de la 300 pour la protection contre les signaux parasites compromettants.
Enfin, le Centre d'études cryptographiques supérieures (sexe comme on l'appelait à l'époque), et son successeur ont formé et forme encore nombre de spécialistes du domaine.

Passons à l'informatique. Au début, les calculateurs sont dans des salles machines où n'entrent que les pupitreurs. La sécurité informatique se résume alors à la sécurité physique des locaux et à l'habilitation des personnels. Les mesures techniques de sécurité se limitent au chiffrement des données échangées.
L'arrivée des ordinateurs multitâches et le déport des terminaux utilisateurs imposent des mesures techniques au cœur des ordinateurs pour contrôler l'emploi des ressources et l'accès à l'information, avec la nécessité d'évaluer leur pertinence.
En 1982, à la création de la DEI et du STEI (conduite des programmes interarmées), je propose à mon futur chef d'étoffer le bureau chiffre et de le placer auprès du département informatique, au lieu du département transmission. Ce fut finalement le département PEI.
Je préside alors un nouveau groupe de coordination entre les services techniques de la DGA, et la DCT et le SERTIM, qui fut baptisé "sécurité des systèmes d'information".

Au milieu des années 80, une profonde réflexion est confiée à la Défense, afin de répondre aux demandes répétées de M. Cattieuw de renforcer les effectifs du Service central.
C'est l'époque où l'EMA rechigne à augmenter les crédits. Peu importe si nous sommes écoutés par les Américains, nous ne pouvons rien faire sans eux, nous n'avons pas d'avions pour projeter nos forces! Convoqué par le DGA pour lui expliquer le domaine, il me soutient que son téléphone du réseau gouvernemental Régis est protégé au niveau Confidentiel Défense. Il n'a pas de cryptophonie, mais l'annuaire papier est tamponné CD!
Englobant les besoins naissants de sécurité informatique, plusieurs décrets du 3 mars 1986 créent une direction interministérielle de la SSI auprès du SGDN, un SCSSI qui lui est rattaché et change le nom du centre de formation. Le SCSSI poursuit la politique et les actions du STCCh dans son ancien domaine du chiffre, pour la sécurité informatique, tout est à faire.

Une première action est de formaliser des critères objectifs d'évaluation des produits et systèmes, et de définir le processus d'homologation.
La sécurité dépasse la confidentialité ; c'est aussi la disponibilité et l'intégrité de l'information, ainsi que l'authenticité de son origine.
Le processus d'homologation/certification distingue 3 intervenants :
- le demandeur de l'évaluation, précise la cible d'évaluation (le périmètre de son produit) et la cible de sécurité (les fonctions du produit et les menaces contrées) ;
- l'évaluateur indépendant examine le produit et sa documentation et rédige son rapport ;
- enfin, l'organisme officiel, le SCSSI pour la France, certifie que la cible d'évaluation fait ce qu'on attend d'elle, avec 2 types d'assurance, l'efficacité des mécanismes (niveau E1 à E6) et la conformité de l'implémentation.
Ce fut le résultat de multiples discussions nationales avec les industriels et l'administration, et de discussions internationales menées en un temps finalement assez bref.

En 1983, la NSA publie son catalogue de critères, pour les besoins du DOD US, le fameux livre orange TCSEC. Bien que très utile, ce document fait la part trop belle à la confidentialité. A l'OTAN, les américains veulent transposer à l'informatique les modalités d'évaluation et d'approbation des machines à chiffrer. Face à cette attitude hégémonique, les principaux pays européens souhaitent définir leur propre document, adapté à leur préoccupation, et confronter leurs réflexions. Apparaissent ainsi en 1989 les documents anglais, allemand et français, les Pays-Bas se joignant aux discussions.

Dès l'origine, les 4 pays recherchent des critères harmonisés valables également pour le commercial et un processus permettant la reconnaissance mutuelle des certificats. Le SCSSI et ses homologues rédigent la version 1 des ITSEC (critères de sécurité des technologies de l'information), qu'ils soumettent à la Commission pour extension à toute l'Union européenne.
Après prise en compte des observations des pays membres, la Commission publie en juin 1991 la version 2 des critères européens ITSEC. Les américains poursuivent le dialogue pour l'adoption de critères communs US-Europe. Le Japon soutient cette action et déclare à l'ISO qu'il se ralliera aux critères communs dès leur publication.

Une action complémentaire très importante est de faire vivre le processus en France, notamment là où nos industriels ont une longueur d'avance sur les autres pays. C'est le cas de la carte à puce, avec le GIE CB comme demandeur et le SEPT de Caen comme évaluateur indépendant.

Le décret confie au SCSSI la mission d'apprécier le niveau de protection des systèmes d'information gouvernementaux et d'approuver leur destination. La demande des ministères se résume souvent à cette simple phrase "mon système est-il bon pour le service?", à laquelle il est impossible de répondre sans connaitre le besoin et les conditions d'emploi.
Pour faciliter le dialogue avec ses correspondants, le SCSSI rédige la FEROS, puis définit la première version de la méthode EBIOS d'Expression des Besoins et Identification des Objectifs de Sécurité ; beaucoup d'entre vous ont utilisé ou utilisent ses versions successives.

Toutes les actions évoquées contribuent à construire un château fort imprenable. La réalité est autre, et au tournant du siècle, le SCSSI s'est adjoint une équipe de sapeurs-pompiers de réponse aux incidents de sécurité, dévolue d'abord à l'administration. Ce fut la création en 1999 du CERT-A, Computer emergency response team.