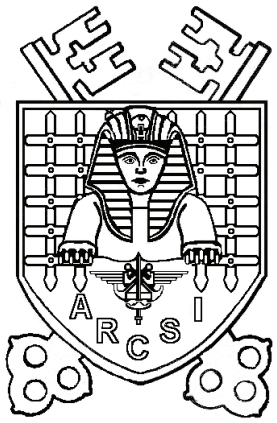

ASSOCIATION des RESERVISTES du CHIFFRE et de la SECURITE de L'INFORMATION

Nouvelle série
n° 28 - 2000

Document interne à l'Association
Réservé aux adhérents

8 . La grande bagarre du Chiffre

Un détail historique.

Chacun sait qu'à Londres, durant la Seconde guerre mondiale, les relations entre les chefs anglais et certains membres de l'état-major des Français Libres n'étaient pas toujours au beau fixe et pouvaient parfois tourner à l'orage.

Le bruit courut un jour, dans les milieux français, que l'Intelligence Service (I.S.) lisait indûment les messages chiffrés du B.C.R.A (Bureau Central de Renseignement et d'Action) parce qu'il en avait "volé les clés". Ce bruit court parfois encore.

Le hasard du service voulut que, dans les années 70, le brigadier NICHOLLS me fît l'honneur de m'inviter chez lui pour passer quelques jours près de Salisbury dans le charmant cottage qui lui avait été donné par le roi en reconnaissance de services éminents rendus au cours des deux guerres mondiales. Je préparais alors une étude sur les moyens techniques du S.O.E (Spécial Opérations Exécutive) en France occupée ; il s'agissait de "parler boutique", l'occasion était inespérée.

Le brigadier Frederick William NICHOLLS (C.B.E, M.B.E, Légion d'honneur plus une Croix de guerre gagnée sur les plages de Dunkerque) devint dans les années 40, le "Directeur du M.1-8" (Département de l'Intelligence Service chargé des interceptions radio et des décryptements à Bletchley Park). Un poste d'une importance considérable dont on ne connaît l'existence et l'organisation que depuis peu. Pour l'état-major des Français Libres 'NIC" n'était que l'officier de liaison britannique chargé des échanges techniques entre les services secrets britanniques et français, un homme de l'ombre sans plus.

En 1970 le vieux brigadier, droit comme une baguette de fusil, représentait l'officier courtois et distingué décrit par André MAUROIS sous les traits de son "Colonel BRAMBLE" célèbre pour ses silences. Son épouse Marjorie, une ancienne capitaine de l'I.S. responsable de l'équipe féminine des "briseurs de codes'" illustrait la politesse et la discrétion de l'ère victorienne. Son thé des Indes, servi dans de la porcelaine chinoise, était infusé à la couleur noble et sa recette de curry succulente. Le brigadier avait fait lui-même le choix des bordeaux en fin connaisseur.

La chaleur des vins et le charme de la vieille demeure aidant nous en étions arrivés à la détermination des dates auxquelles étaient survenus les divers changements des systèmes cryptographiques utilisés par le S.O.E ."NIC" me demanda soudain si j'étais au courant de la "Grande Bagarre du Chiffre" ("The Great Coding Row"). Devant ma réponse négative, il me narra en ces termes les faits suivants :

-"En 1942 nous décryptions pour ainsi dire instantanément tout ce qui était chiffré selon le principe de la double-transposition. Nous dispositions à Bletchley des outils pour le faire. Le problème était infiniment moins ardu que les décryptements des machines allemandes ou italiennes. Sachant que les services du général De GAULLE faisaient un large usage, voire un usage quasi exclusif, de la double-transposition, je demandai un entretien au responsable

français du Chiffre pour lui dire que, puisque nous lisions sans effort les messages allemands chiffrés selon ce procédé, il était raisonnable de penser que nos adversaires pouvaient faire de même. J'exprimai l'idée qu'il serait bon que les services français, à notre image, s'empressent de changer de procédé. Je proposai de leur faire établir des clés aléatoires générées par des machines et microfilmées sur du papier de riz nitraté pour l'utilisation du système dit "à clé une fois".

"Mon interlocuteur fut ce jour là un jeune officier des F.F.L qui, tout en étant fort sympathique, ne me sembla pas avoir de très solides connaissances en cryptographie. Je ne pouvais, bien entendu, rien révéler de ma position réelle ni de l'existence de Bletchley Park où j'avais pourtant sous mes ordres trois brillants cryptanalystes français qui m'avaient été "prêtés pour la durée de la guerre" par mon ami le futur général Bertrand. L'un de ceux-ci n'était autre que le commandant Baudoin.

"Je proposai à mon jeune interlocuteur, afin de le convaincre, de me chiffrer un texte à sa convenance d'une quarantaine de groupes selon la double-transposition et avec ses propres clés. L'offre fut acceptée avec gratitude, mais scepticisme. J'envoyai une estafette qui nous retourna le texte complètement déchiffré dans la demi-heure qui suivit.

"L'officier abasourdi me remercia, salua et prit congé.... Je venais de déchaîner bien involontairement la tempête. Une tempête violente qui remonta au niveau le plus élevé de la hiérarchie et empoisonna nos relations avec l'E.M du B.C.R.A qui nous accusa d'avoir pénétré leurs coffres par effraction et volé leurs clés de transposition.

"Voilà ! vous êtes le seul à connaître le fond de cette malheureuse histoire... Mon unique but était de rendre service à mes collègues français et de leur éviter des pertes prévisibles sur un territoire occupé par l'ennemi. A l'époque je ne pouvais rien dévoiler du grand secret des décryptements, je savais que les Allemands interceptaient et traduisaient les messages chiffrés par les Français : nos interceptions et décryptements de la machine "Enigma" le prouvaient. Hélas ! j'étais tenu par le secret et je souffre toujours de ce malentendu."

Ainsi parla le brave brigadier. Et je revois encore la figure peinée du vieux soldat humilié qui avait été pris pour un vulgaire perceur de coffre, un voleur indigne de la confiance des hôtes qu'il hébergeait...

Cette leçon de cryptographie ne semble pas avoir porté ses fruits puisque je devais découvrir en 1972 un message du S.R français "Kléber" à destination de Londres, daté du 27 août 1944, et donnant des informations concernant le regroupement à Bordeaux du "Reserve Korps 64" et son mouvement vers le front. Ce message, de valeur "A" était chiffré selon la méthode doublement dangereuse de la transposition avec l'emploi d'une clé logique provenant d'une phrase du livre "Servitude et grandeur militaires". Mon ami le colonel de BUTTET, ancien du réseau Kléber, à qui je racontai l'histoire du brigadier me dit n'avoir jamais été mis au courant par sa hiérarchie et confirma que la double transposition, considérée comme sûre à l'époque, était utilisée pour la plupart des messages des réseaux français, par routine, sans réfléchir plus avant.

Je suis le seul témoin de cette révélation du brigadier et si j'ai pu me faire l'interprète posthume de sa tristesse et redresser un tort causé à un grand soldat à qui la France doit beaucoup, je remercie vivement l'A.R.C.S.I. de m'en avoir procuré l'occasion.

Pierre LORAIN