LES MOYENS DE CHIFFREMENT BRITANNIQUES PENDANT LA 2eme GUERRE MONDIALE

Les « Presses de sa Majesté » ont publié récemment un ouvrage du plus grand intérêt : « le renseignement britannique pendant la 2 eme guerre mondiale ». Il s'agit d'une étude approfondie de l'acquisition, de la circulation et de l'exploitation de l'information par les Britanniques durant la guerre 1939-1945.

Cette somme qui comprend 3 tomes de plus de 800 pages chacun a été rédigée par une équipe officielle d'historiens, sous la direction du Docteur HINSLEY.

La prééminence quasi-totale de l'interception radioélectrique et du décryptement, par rapport aux autres sources, est mise en lumière. La plus large place est évidemment donnée aux décryptements des systèmes allemands basés sur l'ENIGMA, mais les autres systèmes sont également mentionnés, en particulier les systèmes tactiques qui, s'ils n'ont pas eu d'impact stratégique, ont eu une grande importance sur le champ de bataille.

Sauf exceptions, les messages ENIGMA, provenant de niveaux assez élevés du Commandement allemand, remis aux Etats-Majors entre 24 heures et quelques jours après leur transmission (souvent même quelques heures pour les messages de la LUFTWAFFE) avaient souvent peu de valeur tactique immédiate. Ainsi durant la bataille aérienne d'Angleterre (été-automne 1940) les messages ENIGMA de la LUFTWAFFE donnaient des indications générales mais non le détail des actions pour lesquelles l'analyse électronique (faisceaux directeurs), les écoutes tactiques et le réseau radar ont joué le rôle majeur.

Il n'est pas possible ici de rendre compte de l'énorme masse d'information que cet ouvrage met à la disposition des historiens, des 2emes bureaux et des Transmissions, avec les

conséquences de toute nature à en tirer pour le présent et l'avenir, mais un aspect particulier mérite l'intérêt des chiffreurs. Une annexe du Tome II donne en effet le détail des moyens de chiffrement utilisés par les Britanniques et de la sécurité vis-à-vis des services de décryptement allemands.

LES MOYENS UTILISES PAR LES BRITANNIQUES

Dans l'ensemble les Britanniques ont utilisé des systèmes à base de codes surchiffrés et la machine TYPEX.

La machine TYPE X, devenue TYPEX est une machine à rotors, inspirée par l'ENIGMA, dont les services Britanniques avaient acheté deux exemplaires (commerciaux) en 1928. Cette machine, adoptée en 1935 par le WAR OFFICE et l'AIR MINISTRY était imprimante (contrairement à l'ENIGMA) et utilisait 5 rotors à avancement non régulier ; elle présentait de ce fait une sécurité élevée et n'a jamais été décryptée par les Allemands.

L'Amirauté demeure en 1935 assez réticente, car les messages obtenus étaient naturellement plus longs que ceux donnés par des codes ; ce n'est qu'à partir de la fin de 1943 qu'elle l'introduisit, sous l'effet de la nécessité.

Les codes à 4 ou 5 chiffres étaient en général utilisés avec un procédé de surchiffrement par clés soustractives longues, extraites de cahiers ou carnets de clés.

La confiance accordée par les Britanniques à ce procédé reposait sur le fait que ces cahiers ou carnets devaient être changés assez fréquemment, compte tenu du volume du trafic, de façon que l'adversaire ne puisse avoir un nombre de messages suffisants pour l'attaquer avec succès (recouvrements, messages stéréotypés). Il apparait que l'Amirauté et le service du chiffre avaient sous-estimé le volume de trafic à prévoir (en particulier pour les convois) et suréstimé l'effet des mesures de silence radio.

La première découverte de la faiblesse de ce système survint pendant la campagne de NORVEGE (1940) : un « énorme » volume d'informations tactiques provenant de décryptements allemands apparut dans les messages ENIGMA, mais on pensa d'abord que ceci était dû à la capture de documents du chiffre dans des sous-marins perdus en janvier 1940 et sur le navire HARDY à NARVIK.

Les Britanniques se rendirent cependant peu à peu à l'évidence, changèrent les codes, accélérèrent les changements de cahiers de clés dans la mesure du possible (problèmes de mise en place, surtout pour la Marine), adoptèrent des procédés plus sûrs de camouflage de l'indicateur de départ (préambules). Mais en fin de compte, ils adoptèrent un dispositif de dérivation de clés, à l'aide d'un appareil conçu en 1941 par le service du chiffre mais dont les problèmes de fabrication, d'emploi, de distribution retardèrent la mise en service jusqu'en juin 1943.

Ils mirent également, en service et de plus en plus des systèmes à clé une fois.

Le détail de l'évolution des moyens est donné dans l'annexe ci-jointe, mais il apparait important d'insister sur un certain nombre de points importants d'un point de vue général pour la sécurité :

- l'évaluation de la sécurité d'un système repose toujours sur un certain nombre d'hypothèses en partie objectives, en partie subjectives : sureté intrinsèque, volume du trafic, règles d'exploitation (marquants), respect des règles par les utilisateurs.

C'est ainsi que les règles d'exploitation de l'ENIGMA présentaient une faille aggravée par le laxisme des opérateurs (marquants stéréotypés) qui permit l'entrée des Polonais dans le système. Une déficience analogue apparut dans le système de camouflage des marquants de messages utilisé avec la machine M 209 par l'Armée de Terre française quelques années après la guerre, fut relevée et heureusement signalée par un sous-officier

chiffreur. Un exemple en est aussi donné en annexe : le chiffre naval n° 2 résista à peu près aux décrypteurs allemands jusqu'en septembre 1941, lorsqu'un nouveau système de marquants assez faible remplaça le précédent (sans doute jugé gênant par les utilisateurs).

- tout système peut présenter une faille ; c'est pourquoi il est essentiel de poursuivre les études de décryptement sur celui-ci et d'en suivre l'emploi, ainsi que d'être à l'affût d'informations même allusives sur sa validité. Les Britanniques eurent le bonheur d'avoir, par le décryptement de l'ENIGMA la source idéale, contrairement aux Allemands qui gardèrent jusqu'au bout leur confiance à l'ENIGMA et à leur téléimprimeur chiffrant grâce notamment aux mesures draconniennes prises par les Anglais et plus tard les Américains pour éviter toute divulgation ou exploitation intempestive (ULTRA).

- l'emploi parallèle de plusieurs systèmes non coordonnés est dangereux, car la connaissance d'un système faible peut ouvrir la voie au décryptement d'un système solide ; ce peut-être le cas d'un simple système de codage ou de camouflage par rapport à un chiffre, d'un chiffre de police par rapport à un chiffre militaire (le cas advint en Allemagne pendant la guerre) et les Britanniques mirent sur pied pour pallier ce risque un « comité interarmées de sécurité du chiffre » en décembre 1940 ; il s'étendit peu après aux Affaires Etrangères, contrôla aussi en septembre 1941 les procédures, s'adjoignit en octobre 1941 les colonies, les Dominions et l'Inde puis devint totalement interministériel en 1943.

Ceci est à rapprocher des dispositions françaises : commissions interministérielles de 1909 et de 1935 qui ne paraissent avoir eu qu'une efficacité réduite, puis direction technique des chiffres (interministérielle) à Alger en 1943, et enfin commission interministérielle des chiffres depuis 1951.

Mais cette coordination ne peut fonctionner que si elle découle d'une autorité majeure (Premier Ministre) et si elle a un support technique permanent.

- enfin disposer à tout moment des moyens de rechange permettant de faire face sans retard à une compromission apparaissant inopinément. L'exemple britannique du remplacement des cahiers ou carnets de clef insuffisants par un dispositif de dérivation conçu en 1941 mais qui ne peut-être mis en service qu'en 1943 le montre bien. Cette faiblesse fut cependant palliée par l'emploi de clés une fois pour les liaisons méritant un degré de protection élevé.

L'ouvrage Britannique n'a donc pas seulement un intérêt capital pour l'histoire de la 2eme guerre mondiale, mais il est riche d'enseignements à appliquer par les 2emes bureaux, en particulier l'organisation du renseignement à tous les niveaux et par les services de sécurité et du chiffre, mais aussi par toutes les autorités ayant une responsabilité : nécessité du renseignement, utilisation de celui-ci, protection du secret.

Il montre notamment que tout investissement dans les domaines du renseignement et de sécurité est payant, et qu'une décision d'économie à court terme (ce fut le cas avant 1939) peut-être catastrophique.

L. RIBADEAU DUMAS