

NOTE HISTORIQUE N°15

L'ÉMERGENCE D'UNE CRYPTOGRAPHIE MILITAIRE EN FRANCE

Gérald Arboit

L'anecdote est connue : le 9 août 1870, lorsque le maréchal François Achille Bazaine, nommé commandant du III^e de l'armée du Rhin, se plaignit de ne pas disposer de moyens de chiffrement, l'état-major de l'Armée ne put lui fournir qu'un vieux code diplomatique, dont le principal inconvénient était de ne pas comporter de vocabulaire militaire¹. Cette anecdote est autant révélatrice de l'état de déclin de la cryptologie française depuis la Révolution que du poids pris par le bureau du Chiffre des ministères des Affaires étrangères depuis 1863 dans la protection des communications gouvernementales et militaires². Elle est néanmoins confirmée par un autre épisode mettant en scène le maréchal Bazaine, enfermé dans Metz cette fois, et tentant d'en informer le gouvernement de la Défense nationale du général Trochu.

« Le 21 [octobre 1870], le maréchal Bazaine tentait, pour la première fois, de correspondre avec le gouvernement de la Défense nationale dont il n'avait jusqu'alors jamais reconnu l'existence. La dépêche chiffrée, qui est parvenue au ministère de la Guerre par les mains de deux officiers de l'état-major général, était conçue dans un chiffre inconnu aux divers départements de l'administration publique.

Par un hasard étrange, sinon par une combinaison machiavélique du maréchal, le chiffre qui avait été employé fut reconnu pour être le chiffre dit impérial, dont la clef ne se trouve qu'entre les mains de l'Empereur ou celles de ses anciens ministres³... »

En entendant ce passage du rapport, M. Crémieux⁴ particulièrement a dû ressentir quelque embarras. Je le vois encore se demandant comment on déchiffrera la dépêche du maréchal.

Il se fait conduire chez la maréchale, espérant qu'elle avait la clef qu'il avait oublié de prendre en partant de Paris.

La maréchale, qui ne peut le satisfaire, s'imagine que je trouverai un moyen de le faire. Elle

¹ André Catthiew, « La cryptologie française », Pierre Lacoste (dir.), *Le Renseignement à la française* (Paris, Economica, 1998), p. 291.

² Cf. Gérald Arboit, « La fin d'un monde : le bureau du chiffre du Quai d'Orsay en 1904 », CF2R, *Notes historiques*, janvier 2008, <http://www.cf2r.org/fr/notes-historiques/la-fin-un-monde-le-bureau-du-chiffre-du-quai-orsay-en-1904.php>.

³ Rapport du chevalier, vicomte de Valcourt, se présentant comme l'officier d'ordonnance du maréchal Bazaine (alors qu'il n'était qu'un interprète attaché du général Blanchard), à Gambetta, ministre de l'Intérieur, du 28 octobre 1870.

⁴ Isaac-Jacob, dit Adolphe, Crémieux était ministre de la Justice, garde de Sceaux. Depuis le décret du 16 septembre 1870, il détenait « la délégation du gouvernement de la Défense nationale, appelée à exercer les pouvoirs de ce gouvernement dans les départements non occupés par l'ennemi », depuis le siège du gouvernement à Tours.

monte dans le coupé de M. Crémieux, et les voilà tous deux à ma recherche. Ils me rencontrent en ville, font arrêter la voiture, et ils m'expliquent l'embarras de la Délégation. Si M. le général de Noue¹, ancien chef d'état-major général au Mexique, se fût trouvé à notre portée, il aurait pu reconnaître peut-être que le chiffre était le même que dans l'expédition du Mexique; mais le général était à Paris.

On ne put donc à Tours déchiffrer la dépêche du maréchal, pour avoir oublié la clef du chiffre. Cette dépêche fut portée à Paris par M. Thiers, je crois, et au ministère de la Guerre on la traduisit immédiatement.

Elle ne revenait à Tours que le 17 décembre suivant, à cause des difficultés de communication². »

Ce désordre est certes symptomatique d'une nation en déliquescence, qui a changé de régime en plein conflit extérieur (4 septembre), et dont on peut en trouver trace dans les ressentiments de l'auteur de cette relation. Pourtant, ces problèmes cryptographiques de campagne touchaient toutes les armées, y compris (et peut-être même surtout) les contingents allemands. Certes, leur haut commandement faisait une meilleure utilisation pour leurs communications de l'invention du télégraphe, dont il avait pu observer les effets durant la guerre de sécession américaine, comme le démontra brillamment l'*Hauptmann* Max Hering³. Mais il ne se préoccupait guère plus de leur protection, et il s'agissait là d'une constante européenne. Si la création d'un bureau de Déchiffrement au ministère français de la Guerre trouvait naturellement son origine dans la défaite, elle n'en était pas moins le fruit d'une double évolution typiquement française. D'une part, l'éclosion d'une école française de cryptologie joua un rôle évident dans son établissement. Mais il fallait aussi y voir les conséquences de l'Affaire Dreyfus.

Des réflexions en marge de celles sur la constitution d'un appareil de renseignement

Les années consécutives de la défaite furent en France l'occasion d'un foisonnement intellectuel autour de la nécessité d'une transformation totale de l'outil militaire. Transparaissait parfois une volonté de créer un service permanent de renseignement militaire⁴. Ses plus grands thuriféraires étaient des officiers issus du Dépôt de la Guerre du Second Empire, commandé par le général Jarras. Ils avaient été envoyés en reconnaissance à la frontière de l'Est dès la mobilisation et avaient pu constater « l'insuffisance en France d'un mécanisme qui n'était même pas prévu »⁵. Ils s'agissaient bien sûr du lieutenant-colonel Fay et du capitaine Jung⁶, mais également des commandants Vanson, Samuel et Championnet. Mais la figure tutélaire du colonel Jules Lewal⁷ émergeait le plus, prônant notamment l'avènement d'une

¹ Il s'agit en fait du chef d'escadron d'artillerie Ludovic de Noüe (1829-1887), officier d'ordonnance du général Bazaine pendant l'expédition (1861-1866). En octobre 1870, il commandait l'artillerie de la 2^e division d'Infanterie (les 19^e batterie du 9^e régiment, et 5e et 6e batteries du 12^e régiment) de l'armée de la Loire. Promu colonel le 8 octobre 1875, il ne devint général que le 22 août 1882, avant d'être placé en 2^e section le 9 décembre 1886.

² Maurice d'Irisson, comte d'Hérisson, *La légende de Metz*, 3e éd. (Paris, Paul Ollendorf, 1888), p. 274-275.

³ « German Signal-Communications in 1870 », *Army Quarterly*, n° 21, octobre 1930, 138 pages.

⁴ Cf. notamment Jules Lewal, *La réforme de l'armée* (Paris, Librairie militaire Dumaine, 1871) ou Charles Fay, *Projet de réorganisation de l'armée française* (Tours, Mame & fils, 1871).

⁵ Service historique de la Défense (SHD)/Département de l'Armée de terre (DAT), 1 K 732, lettre du capitaine Henri Jung au général François Renson d'Allois d'Hercule du 24 mai 1873.

⁶ Ernest Alfred Vizetelly, *My days of adventure : the fall of France (1870-71)* (Londres, Chatto and Windus, 1914), p. 43.

⁷ SHD/DAT, 7 Yd 1616.

cryptographie française. L'adjoint de Jarras déplorait qu'un système « d'un emploi facile et sûr [était] une lacune, qui a toujours existé dans notre armée »¹.

En 1881, devenu général et auteur prolifique d'« Etudes de guerre », il publiait *Tactique des renseignements*² et consacrait un chapitre à la cryptographie résumait ses connaissances en la matière. Ce défaut initial de maîtrise technique l'amena certes à rédiger des propos discutables. Mais il n'en manqua pas moins d'apporter, dans ce domaine également, des lumières nouvelles. Abordant la définition d'un chiffre militaire et de ses besoins en temps de guerre (plusieurs chiffres pour chaque niveau hiérarchique), il rappelait le besoin d'en imposer l'usage systématique dans l'armée et de former les officiers à ses méthodes.

Mais le souci des militaires n'en étaient pourtant pas encore arrivé à assurer la protection des communication. Le retour d'expérience du siège de Paris, malgré la dérivation du câble de Seine — et donc l'écoute — par les Prussiens, n'avait pas été mené complètement et le système avait été jugé sûr³. L'heure était à la mise en place des fonctions spécialisées de recherche et d'exploitation du renseignement. La première incombait à la nouvelle « statistique militaire et travaux régimentaires » créée au sein de l'« état-major général du ministre de la Guerre », institué par le décret du 12 mars 1874. Quant à la seconde, elle dépendait du Deuxième bureau de l'état-major. Pour bien signifier la distinction entre ces deux fonctions, le décret de 1874 plaçait la section de statistiques, nom qu'elle ne prit qu'officiellement avec la nomination du commandant Sandherr, en décembre 1886⁴, directement sous les ordres du sous-chef d'état-major coiffant les Premier et Quatrième bureaux.

Pourtant, le développement mondial de la télégraphie électrique ne tarda pas à susciter un intérêt grandissant pour la cryptographie. Moyen de communication ouvert — les dérivations étaient aisées —, mais cher — le paiement s'effectuait à la lettre —, les utilisateurs publics et commerciaux — banquiers et commerçants — avaient retrouvé les bienfaits de la correspondance chiffrée. Exigence de confidentialité autant que de condensation des télégrammes, donc de coût, des dictionnaires remplaçant mots et phrases par des groupes de chiffres, furent bientôt édités⁵. Ils suivaient en cela l'évolution de la réglementation depuis 1865 ; la loi du 13 juin 1866 accorda au public la faculté de correspondre en chiffres sur le territoire français, quand la convention de Saint-Petersbourg, du 10 au 22 juillet 1875, permettait même l'emploi d'une correspondance chiffrée pour les communications télégraphiques internationales. L'objectif était plutôt de garantir une confidentialité vis-à-vis des Britanniques sur les lignes transatlantiques que de se prémunir contre tout espionnage. Dès 1868, était publié le Sittler Les principaux gouvernements européens commencèrent à équiper leur diplomatie avec des systèmes fiables, forcément secrets, mais en conformité avec les normes internationales. En outre, le

¹ *Etudes de guerre*, III, *Tactique de marche* (Paris, Librairie militaire Dumaine, 1876), <http://gallica2.bnf.fr/ark:/12148/bpt6k86125p.modeAffichageimage.r=lewal.f1.langFR>.

² Général J. Lewal, *Tactique des renseignements*, « Etudes de guerre », Paris, Baudoin, 1881, 2 volumes.

³ F. Lacombe, « Les transmissions pendant le siège de Paris 1870-1871 », *Revue Historique de l'Armée*, n° 4, novembre 1966, pp. 113-133.

⁴ SHD/DAT, 1 K 171 et général André Bach, *L'armée de Dreyfus. Une histoire politique de l'armée française de Charles X à « l'Affaire »* (Paris, Tallandier, 2004), p.540.

⁵ Parmi les plus importants, on notera ceux F. J. Sittler, *Dictionnaire abrégé chiffré* (Paris, A. Augros, 1868), Brunswick, *Dictionnaire pour la correspondance télégraphique secrète, précédé d'instructions détaillées et suivi de la convention télégraphique internationale conclue à Rome le 14 janvier 1872, par un secrétaire de légation* (Paris, 1868), Mamert-Gallian, *Dictionnaire télégraphique économique et secret* (Paris, Plon, 1874). Les dictionnaires portugais de Vaz Subtil (Lisbonne, 1871), allemands de Niethe, (Berlin, 1877) et de Walert (Winterthür, 1877), ou anglais de Bolton reposaient sur le même principe. M. Louis, le directeur du *Journal des Postes*, publia également un *Dictionnaire pour la correspondance secrète* (Paris, 1881).

recours à la télégraphie imposait de revoir les méthodes de chiffrement. Techniquement, l'intermédiation de l'alphabet Morse interdit l'utilisation de symboles graphiques, dont l'usage était largement répandu dans le chiffrement traditionnel, et imposait d'inventer des systèmes compatibles.

Les militaires et la cryptologie

En 1883, un linguiste de l'École des hautes études commerciales prenait le risque de répondre aux arguments du général Lewal en matière cryptographique. Auguste Kerckhoffs apportait la connaissance technique qui manquait à l'officier et fournissait une définition plus complète du chiffre militaire, ne manquant pas de contester et nuancer les propos du général Lewal. Par sa clarté, la qualité de ses sources, la valeur des systèmes de chiffrement qui y sont exposés et la pertinence des analyses de l'auteur, *La cryptographie militaire* s'impose comme un ouvrage de référence, qui est à l'origine d'un véritable renouveau des études cryptographiques¹.

Ce véritable état de la science cryptographique fut bien reçu dans la petite communauté de cryptographes français. Il entraîna même une émulation, au point de provoquer un véritable renouveau de cette science et l'éclosion d'une véritable « école française »². Kerckhoffs lui ayant donné un ton particulièrement passionnel, cet engouement ne manqua pas de le conserver. En vingt ans, il se publia en France vingt-neuf livres sur le sujet, contre seulement six en Allemagne³. Le résultat en fut une confortable avance sur ses principaux voisins, aussi bien la Grande-Bretagne que l'Allemagne. Il fut aussi de donner corps « à une définition moderne de la cryptologie, où les deux branches – chiffrement et déchiffrement – sont finalement définies »⁴.

Les militaires n'étaient pas en reste. Seulement, ils en étaient encore à s'interroger sur l'usage du télégraphe. Depuis l'été 1875, l'administration des Postes et télégraphes fournissait au ministère de la Guerre⁵, comme elle le faisait d'ailleurs pour le bureau du Chiffre des Affaires étrangères, les copies de tous les télégrammes chiffrés le concernant. Comme ils étaient réservés à un nombre restreint d'utilisateurs en dehors du ministre, du chef d'état-major et des commandants de corps d'armée, cette pratique suffisait à occuper à l'état-major général un officier au sein du bureau du courrier. Ce qui n'était pas sans provoquer quelques fois des inconvénients. Ainsi, à l'été 1877, « pendant la guerre turco-russe on reçut, un dimanche, d'un des attachés militaires qui suivaient les opérations des armées en lutte, une dépêche

¹ *La cryptographie militaire ou des chiffres usités en temps de guerre* (Paris, Dumains, 1883). Il avait testé au préalable ses théories dans un article en deux parties, « La cryptographie militaire », publié dans *Journal des sciences militaires*, vol. IX, de janvier, pp. 5-38, et février 1883, pp. 161-191. Ce professeur d'allemand se tourna ensuite vers le volapük (1885).

² Cf. Hippolyte Désiré Josse, *La cryptographie et ses applications à l'art militaire* (Paris, Baudoin, 1885) ; De Viaris, « Variétés : Cryptographie », *Génie civil*, 8^e année, tome XIII, 2^e semestre 1888, n° 2-7, pp. 24-27, 38-39, 55-56, 72-75, 84-88, 104-107 ; Marquis de Viaris, *L'art de déchiffrer les dépêches secrètes* (Paris, Gauthier-Villars et fils, G. Masson, 1893) ; Paul Valerio, *De la cryptographie. Essai sur les méthodes de déchiffrement* (Paris, Baudoin, 1893) ; Commandant E. Bazeries, *Les chiffres secrets dévoilés* (Paris, Fasquelle, 1901) ; Félix-Marie Delastelle, *Traité élémentaire de cryptographie* (Paris, Gauthier-Villars, 1902)

³ Christopher Andrew, « Déchiffrement et diplomatie : le cabinet noir du Quai d'Orsay sous la III^e République », *Relations internationales*, n° 5, 1976, p. 44.

⁴ Alexandre Ollier, « L'essor de la cryptologie française entre 1880 et 1914 », Ministère de la défense, Centre d'études d'histoire de la défense, *Des réseaux et des hommes. Contributions à l'histoire du renseignement* (Paris, L'Harmattan, 2000), p. 16. Cf. aussi l'édition de son mémoire de maîtrise, Paris IV-Sorbonne, *La cryptographie dans l'armée française 1881-1914* (Panazol, Lavauzelle, 2002).

⁵ En outre, cette administration était chargée de la mise sur pied, en cas de mobilisation, des unités de télégraphie militaire.

chiffrée qui, par suite de l'absence du chef de bureau chargé de la correspondance cryptographique, ne put être déchiffrée. Le Ministre, qui ignorait la clef de la dépêche, ne crut alors pouvoir mieux faire que de prier un des officiers de l'état-major d'en essayer le déchiffrement sans clef : au bout de quelques heures le cryptogramme était traduit ! Heureusement pour le secret de la correspondance, l'habile déchiffreur était le fils du Ministre lui-même »,¹ le lieutenant Henry Berthaut. Cet officier d'état-major quitta le ministère peu après le départ de son père et ne poursuivit pas dans l'art cryptographique, mais plutôt dans celui de la géographie militaire².

*Présidents de la commission et inspecteurs généraux de la télégraphie militaire*³

Nom	Prénoms	Entrée en fonction
Gresley	Henry-François-Xavier	21 février 1872
Schmitz	Isidore-Pierre	29 novembre 1873
Nugues	Saint-Cyr-Louis, Baron	3 mars 1879
Saget	Henri	30 mars 1881
Andlau	Joseph d'	22 décembre 1881
Boquet	Louis-Henri	23 avril 1882
Boudet ⁴	Pierre-Antoine-Bruno	1 ^{er} mars 1886
Gillon	Jean Baptiste Alexandre	1 ^{er} juillet 1890
Peaucellier	Charles-Nicolas	20 février 1891
Adorno de Tscharner ⁵	Antoine-Charles	21 octobre 1888
Lepus	François-Ernest	28 décembre 1889
Moutz	Marius-Stanislas-Philomin	11 juillet 1882
Niox	Gustave-Léon	8 juillet 1893
Correnson	Louis-Marie-Rodolphe-Achille	28 septembre 1893
Borius	Léon-Charles	16 juin 1897
Penel	François	31 janvier 1899
Quinivet	Hubert-Antoine	3 juin 1899
Derendinger	François-Ignace	1 ^{er} juillet 1900
Roux	Edouard-Gabriel-Georges	12 août 1902
Petit	Pierre-François-Joseph	12 mai 1903
Joly	Edouard-Léon	24 décembre 1904
Vieillard	Ernest-Antoine	20 février 1908
Marcy	Henri	4 février 1910
Delarue ⁶	René-Joseph	8 novembre 1910

¹ Auguste Kerckhoffs, « La cryptographie militaire », *Journal des sciences militaires*, vol. IX, janvier 1883, p. 10.

² SHD/DAT, 9 Yd 484.

³ *Ibid.*, 7 N 1971 et 9 N 63.

⁴ Il occupa également la vice-présidence de la commission du 27 juillet 1886 au 6 octobre 1887 [SHD/DAT, 10 Yd 94].

⁵ En italique et en alinéa figurent les inspecteurs généraux des services de la télégraphie militaire.

⁶ Il assura à partir de 1913 les fonctions de l'inspecteur technique des troupes du Génie autre que le Génie des places, des chemins de fer et des télégraphistes [9 Yd 501].

Du côté de la Commission de télégraphie militaire, recrée fin février 1872, aucune avancée notable n'était à entendre. De 21 février 1872 au 2 août 1914, dix-huit présidents se succédèrent, soit un mandat moyen de quelque trois ans et demi. Choisis parmi des généraux de division du Génie à compter de 1891, ils avaient en moyenne 57 ans ; on constate à partir de 1897 un vieillissement, puisque les neuf derniers avaient la soixantaine. Cinq généraux accomplirent au moins deux ans, quatre ne restèrent pas plus de neuf mois et quatre trois ans ; seuls cinq dépassèrent trois ans, dont deux presque six ans ; le baron Nugues et Boquet connurent les plus longs mandats. Toutefois, cette présidence apparaissait comme n'être que symbolique, les généraux du génie qui l'occupèrent cumulant avec d'autres fonctions, aux comités consultatif ou technique d'état-major et/ou du génie, ainsi qu'à la commission mixte des Travaux Publics. S'ajoutaient encore des fonctions militaires, en région jusqu'en 1881 puis, à compter de 1893, de commandement du Génie du gouvernement militaire de Paris. A partir de 1893, la commission de télégraphie devint consultative et son président prit également en charge la commission d'aérostation militaire. La commission de télégraphie tenta vainement de se saisir de la question cryptographique¹, mais l'instabilité et la superficialité de ses débats n'arrivèrent à rien produire.

La nomination d'un inspecteur général des services télégraphiques, à compter de 1886, signifiait que l'utilisation de ce mode de communication s'était répandu dans les armées françaises, comme en attestait déjà sa prise en charge par le Quatrième bureau de l'état-major général. Comme les personnels étaient insuffisamment qualifiés, une école de formation avait été installée à Suresnes, dans le grand fort du Mont-Valérien, en raison des capacités de transmission optique offertes. En 1888, les Invalides accueillirent la direction de cette nouvelle arme en devenir. Deux ans plus tard, s'y ajoutait un dépôt central...

Choisis parmi les généraux de brigade² d'état-major, puis d'infanterie, ou du Génie, les inspecteurs généraux des services télégraphiques étaient membres du comité technique d'état-major et de la commission mixte des Travaux publics à partir de décembre 1889. Dans ce milieu se développa une réflexion sur l'utilisation de la cryptographie. Par leurs fonctions, les inspecteurs étaient les mieux placés pour se rendre compte combien les mesures adoptées dans l'urgence pour assurer la sécurité des communications militaires en opération s'avéraient insuffisantes³. Un premier point portait sur le renforcement de la formation des personnels. La vieille croyance qu'il ne suffisait que de manipuler les dictionnaires de code pour chiffrer un texte entraînaient d'innombrables erreurs. Il convient de préciser que, malgré les apparences⁴, toutes les armées européennes connaissaient les mêmes balbutiements. Les états-majors considéraient que l'emploi de la cryptographie ne nécessitait aucune

¹ Cf. le *Bulletin officiel du ministère de la Guerre* du 1^{er} semestre 1890, pp. 845-847.

² Exception faite du général Delarue, qui cumulait les fonctions de président de la commission et d'inspecteur général des services télégraphiques, seul Gustave-Léon Niox fut promu, le 24 octobre 1899, général de division. Ce qui lui permit de quitter l'inspection pour d'autres commandements dans l'infanterie. Placé dans le 2^e section des officiers généraux, le 8 août 1905, il prit le commandement de l'établissement des Invalides et la direction du Musée de l'Armée, qu'il abandonna à l'âge de 79 ans, le 1^{er} décembre 1919 [SHD/DAT, 9 Yd 303].

³ Cf. « La sécurité des transmissions du corps expéditionnaire du Tonkin en 1885 », *Revue des Transmissions*, novembre-décembre 1959, n° 87, pp. 9-12.

⁴ Auguste Kerckhoffs notait ainsi en 1883 que « les Allemands posent en principe que la correspondance cryptographique doit être employée de la manière la plus étendue ; les programmes de leurs écoles militaires prescrivent non seulement d'exercer les officiers à la composition et à la lecture des dépêches secrètes, mais encore de les initier à la connaissance de tous les principes théoriques de l'art de déchiffrer. L'article 32 du règlement du 19 janvier 1874 porte également que les dépêches militaires doivent, autant que possible, être chiffrées » [op. cit., p. 5].

formation¹. Bien sûr, grâce à l'intérêt du général Lewal et du baron Nunge, le cours de service d'état-major de l'École supérieure de guerre abordait tout de même la question, mais dans une rapide présentation des grands principes de cryptographie. L'écart était cependant réel si l'on comparait l'état de la cryptographie militaire à ce qui se faisait dans le monde commercial français.

Les inspecteurs étaient également à même de détecter au sein des rangs les personnalités conscientes des faiblesses françaises et soucieuses de les corriger. Le capitaine Etienne Bazeries² le fut, au printemps 1890, lorsqu'il déclara le système cryptographique modèle 1886 décryptable. Cet amateur de cryptogrammes qui paraissaient dans la presse était alors en poste à l'état-major du 11^e corps d'armée, basé à Nantes. Intrigué, son nouveau supérieur, le général Fay, le met à l'épreuve, avant de signaler ses talents de cryptanalyse au ministre de la Guerre. La commission de télégraphie fut réunie pour la première fois afin de se saisir d'un problème de cryptographie. Elle décida de modifier le procédé 1886 afin de le rendre plus fiable. Avant même sa mise en œuvre officielle, Bazeries ruina les illusions de ses concepteurs. Nouvelle réunion de la commission qui déboucha sur la création de deux dictionnaires de chiffrement, dits « modèle 1890 type I » pour le temps de paix, et « modèle 1890 type II » pour le temps de guerre.

Alors que le succès de Bazeries, et de quelques autres³, commençait à sourdre hors du domaine militaire⁴, ce dernier sembla rester sourd à son talent. Il fallut encore quatre années avant que le ministre de la Guerre décida d'étendre l'usage de la correspondance chiffrée et chargea une commission de rechercher un procédé de chiffrement sûr. En 1894, cette création d'une commission de cryptographie militaire constituait une étape majeure, après la décision de 1890, même si sa mise en place se faisait sur le modèle « consultatif » de celle de la télégraphie : elle n'était pas permanente, manquait de moyens, à commencer par humains, les personnels siégeant en plus de leur service normal. De fait, aucune continuité du travail n'était assurée, d'autant que son effectif théorique de huit officiers était fréquemment bouleversé par des mutations⁵. Toutefois, la commission permit de notables avancées. Un après sa création, un dictionnaire chiffré pour les autorités du 2^e degré, ainsi qu'une première note sur le fonctionnement de la correspondance chiffrée dans l'armée étaient rédigés. Quatre ans plus tard, en 1899, deux dictionnaires à l'usage des hautes autorités venaient remplacer ceux de 1890.

¹ Les Allemands le croyaient encore pendant la Première Guerre mondiale, comme le démontrent les affaires du télégramme Zimmermann et Mata-Hari [Cf. Markus Pöhlmann, « German Intelligence at war 1914-1918 », *The Journal of Intelligence History*, hiver 205, vol. 5, n° 2, p. 45]. Quand aux capacités britanniques, elles étaient « médiocre[s] — c'est-à-dire normale » [John Ferris, « Connaissances, influence et pouvoir : les services de renseignements britanniques et la Première Guerre mondiale », Frédéric Guelton, Abdil Bicer, *Naissance et évolution du renseignement dans l'espace européen (1870-1940). Entre démocratie et totalitarisme* (Vincennes, SHD, 2006), p. 101].

² SHD/DAT, 6 Yf 5578, et David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (New York, Scribner, 1996 ; 1^{re} éd. 1967 ; trad. fr. *La guerre des codes secrets*, Paris, Inter Editions, 1977), pp. 244-249. Cf. aussi Candela, Rosario. *The Military Cipher of Commandant Bazeries* (New York: Cardanus Press, 1938).

³ Comme ces deux artilleurs, le chef d'escadron Gaëtan Henri Viarizio (de Viaris) di Lesegno et le capitaine Paul Valerio [David Kahn, *op. cit.*, p. 240-242 et Gérald Arboit, *op. cit.*].

⁴ Cf. la présentation de ses travaux par le mathématicien Etienne Lucas lors du congrès de l'Association française pour l'avancement des sciences à Marseille de 1891 [Charles-Ange Laisant, *Sur Arithméticien* (Amiens, Impr. Yvert et Tellier, 1907), pp. 6 et 20] ou sa mise à disposition du ministère des Affaires étrangères à deux reprises pendant son service actif (du 22 août 1891 au 26 octobre 1893, et du 29 septembre 1894 au 26 février 1895), puis après son départ en retraite, en février 1899 jusqu'en 1924.

⁵ Cf. Alexandre Ollier, *op. cit.*, p. 18.

Du contre-espionnage au chiffre

Les contre-coups de l’Affaire Dreyfus allaient favoriser une nouvelle avancée. Les accusations à l’encontre du capitaine avaient été permises par une double évolution du renseignement français. Depuis l’arrivée du commandant Nicolas Jean Robert Conrad Sandherr¹, la section de statistique avait prit un inquiétant tournant en faisant du contre-espionnage sa mission principal². Quand aux progrès de la cryptoanalyse, ils avaient bénéficié aux Affaires étrangères et à la Sûreté générale, plutôt qu’aux armées. Dans le cas des charges portées à l’encontre d’Alfred Dreyfus, le télégramme de l’attaché militaire italien, le lieutenant-colonel Alessandro Panizzardi, au général chef d’état-major Nicola Marselli intercepté le 2 novembre 1894 et les débuts de déchiffrement, quatre jours plus tard³, par les hommes de bureau du Chiffre du Quai d’Orsay avaient été déterminants. L’ébauche du 6 novembre 1894 ayant servi à condamner le capitaine Dreyfus, Maurice Paléologue, délégué par le ministère des Affaires étrangères lors du procès en cassation et au conseil de guerre de Rennes, fut amené à en démontrer sa fausseté le 27 avril 1899⁴. Cette déposition avait été précédée par un violent échange de lettres entre février et mars 1899, entre les deux ministres de la Guerre et des Affaires étrangères ; rien qu’entre le 9 et le 27 février, ils s’échangèrent trois missives⁵.

Elle acheva de consommer la lente rupture entre les deux administrations. Privé du secours du Quai d’Orsay pour ses déchiffrements, notamment à destination de la section de Statistique, le 14 avril 1899, Charles Louis de Saulces de Freycinet avait pris un arrêté créant, au ministère de la Guerre, un bureau de Déchiffrement, servi par deux officiers de réserve et rattaché au service de renseignement, auquel était adjoint l’Ecole de télégraphie militaire du Mont-Valérien, pour la métropole, et une section spéciale de l’Ecole du Génie en Afrique du Nord. Las, quinze jours plus tard, le président du Conseil, qui était aussi ministre de l’Intérieur, attribuait, par la circulaire du 1^{er} mai, la responsabilité du contre-espionnage à la Sûreté. Un semaine après, Charles Dupuy le remplaçait par l’éphémère Charles Camille Julien Krantz (un mois et six jours). Pierre Waldeck-Rousseau, nouveau président du Conseil et ministre de l’Intérieur, comme son ministre de la Guerre, le général marquis Gaston Alexandre Auguste de Galliffet, prince de Martigues, achevèrent d’enterrer le bureau de Déchiffrement, en la privant de moyens, avant de rattacher la section de Statistique, rebaptisée section de Renseignements au Deuxième bureau.

A l’occasion de la loi du 24 juillet 1900, réformant la télégraphie militaire⁶,

¹ SHD/DAT, Mi Affaire Dreyfus, bobine 4(3), dossier de pension de Sandherr.

² Cf. Gérald Arboit, « L’affaire avant l’Affaire : le discrédit du colonel Vincent, chef de la section de statistique de l’état-major de l’armée », CF2R, *Notes historiques*, juin 2008, <http://www.cf2r.org/fr/notes-historiques/l-affaire-avant-affaire-le-discredit-du-colonel-vincent-chef-de-la-section-de-statistique-de-etat-major-de-ar.php>.

³ Les hommes des Affaires étrangères n’achevèrent leur entreprise que le 10 ou le 13 novembre 1894 [Joseph Reinach, *Histoire de l’Affaire Dreyfus*, I, 1894 (Paris, La Revue blanche, 1901), pp. 243-251. Cf. aussi le dossier Dreyfus aux AMAE, CPC, Allemagne, NS 53-59], sans que ceux de la section de Statistique n’y portassent quelque attention. Pour eux, le capitaine Dreyfus était le traître recherché.

⁴ Maurice Paléologue, *Au Quai d’Orsay à la veille de la tourmente. Journal, 1913-1914* (Paris, Plon, 1947), pp. 185-186.

⁵ AMAE, Affaires politiques, C-Administrative, 180 et Centre des Archives diplomatiques de Nantes, Correspondance interministérielle, correspondance échangée avec le ministère de la Guerre, 312. Cf. aussi Maurice Paléologue, *Journal de l’affaire Dreyfus 1894-1899. L’affaire Dreyfus et le quai d’Orsay* (Paris, Plon, 1953), pp. 176-177.

⁶ Elle portait aussi création d’un bataillon de télégraphistes militaires à six compagnies rattaché au 5^e régiment du Génie. Transformé par la loi du 30 mars 1912 en un régiment prenant le numéro 8, il comprenait une compagnie de sapeurs-conducteurs, un groupe de sapeurs-télégraphistes des places

l'inspecteur général François Penel prenait la présidence de la commission de cryptologie militaire en crise. Elle n'était plus composée que de quatre membres, dont certains avaient des difficultés à assister aux réunions en raison de leurs emplois du temps chargés. Deux ans plus tard, le colonel Henry-Marie-Auguste Berthaut le remplaçait. Sur l'idée du lieutenant Cartier, la commission se mit alors à rechercher des officiers de la garnison de Paris, afin de reconstituer un bureau de Déchiffrement pour le temps de guerre. Cinq candidats furent finalement retenus en 1903. Le ministre, le général Louis Joseph André, n'en accepta dans un premier temps que trois, dont le commandant Anatole-Paul-Louis-Michel Thevenin et le capitaine Marcel Givierge, qui intégrèrent la commission. Les lieutenants Bassières, Paulier, Latreille et même deux officiers interprètes, Schwab et Freyss, vinrent rapidement les rejoindre¹. Ils formèrent, sous la direction du capitaine Cartier, le noyau du bureau, que d'aucun considèrent comme l'acte fondateur de la cryptologie militaire française.

La commission de cryptologie en 1900

Noms	Prénoms	Grade	Arme	Fonctions
Brun	Jean-Jules	colonel	artillerie	Professeur à l'École supérieure de Guerre
Berthaut	Henry-Marie-Auguste	colonel	Etat-major, puis infanterie	Chef de la section de cartographie du Service géographique de l'armée
Josse	Hippolyte Désiré	colonel	artillerie	
Cartier	François	lieutenant	Génie	Secrétaire de la commission

Pourtant, les moyens accordés par l'état-major s'avèrent toujours aussi insuffisants, contraignant les méthodes à rester sommaires ; le problème des mutations continua à se faire sentir jusqu'en août 1914. De manière générale, les membres de la commission étaient en butte à l'hostilité tant de leurs supérieurs, qui n'appréciaient pas de voir leur personnel mobilisé par ces activités annexes, que des hommes du Deuxième bureau qui les raillaient ouvertement². Cela ne empêcha pas la commission de poursuivre leur mise en place d'un bureau de Déchiffrement pour le temps de guerre. Entre 1899 et 1914, ils produisirent de nouveaux dictionnaires chiffrés, rédigèrent de nouvelles instructions sur le fonctionnement de la correspondance chiffrée³ et inventèrent de systèmes de chiffrement dits SD ou « sans

fortes et treize compagnies de sapeurs-télégraphistes dont une à composition spéciale affectée à la radiotélégraphie. Étaient en outre créés pour l'Afrique du Nord, trois compagnies de sapeurs-télégraphistes, dont une radio, et un groupe de sapeurs-télégraphistes des réseaux d'Afrique du Nord. Son décret d'application du 21 janvier 1901 créa en outre un bataillon de sapeurs aérostiers rattaché au 1^{er} régiment du Génie.

¹ Edmond Lerville, *Les cahiers secrets de la cryptographie. Le Chiffre dans l'histoire, des histoires du Chiffre* (Monaco, Le Rocher, 1972), p. 175 et Olivier Lahaie, *Renseignements et services de renseignements en France pendant la guerre de 1914-1918 : 2^{ème} bureau et 5^{ème} bureau de l'Etat Major de l'Armée 2^{ème} bureau du G.Q.G. (section de renseignement, section de centralisation des renseignements). Evolutions et adaptations*, Doctorat, Histoire contemporaine, 3, Paris IV, 2006, p. 1866.

² Georges Ladoux, *Les chasseurs d'espions. Comment j'ai fait arrêter Mara-Hari* (Paris, Le masque, 1932), p. 135.

³ La « note secrète sur l'organisation de la correspondance chiffrée dans l'armée » du 29 novembre 1912 [cf. SHD/DAT, 7 N 10, édition du 11 mars 1914], la « note pour l'état-major général de l'Armée et les directions du ministère de la Guerre relative aux attributions de la section du chiffre » du 12

dictionnaire ». Des postes de télégraphie sans fil furent également implantés sur le territoire national¹, mais aussi de celui des alliés de la France ; en mars 1911, le lieutenant-colonel Dupont, nouveau chef de la section de Renseignements², se rendit à Folkestone pour officialiser la collaboration cryptographique avec la Grande-Bretagne³.

Trois impulsions décisives furent encore données à la commission pour l'établissement d'un système de cryptologie militaire intégré. En octobre 1903, la première incombait au capitaine Cartier, détaché à la section de Renseignements. Suite à la brouille avec les Affaires étrangères, les militaires se trouvaient privés des télégrammes diplomatiques chiffrés. En mettant en place une coordination des interceptions depuis les postes de radiotélégraphie d'Afrique du Nord, mais aussi de la marine écoutant les communications en Méditerranée, il permit deux avancées notables : dans un premier temps, il amena la commission à s'engager activement dans la voie des déchiffrements⁴, mais il permettait à terme un recueil d'information sur la Méditerranée que la section de Renseignements pouvait utiliser.

La seconde mit plus de temps à voir le jour, tant les conséquences de l'Affaire Dreyfus étaient fortes. L'unique espoir de la commission de cryptographie militaire de réaliser une surveillance cohérente de la correspondance télégraphique résidait en un retour à un *statu quo ante*. Un accord avait bien été trouvé sur la création d'un service de lecture et de contrôle chargé de la censure des télégrammes à la mobilisation. Mais il importait d'établir immédiatement une coordination au moyen d'une commission interministérielle⁵. Les Postes et télégraphes et l'Intérieur acceptèrent, mais pas les Affaires étrangères. En janvier 1909, un décret présidentiel officialisait sa création. Il s'agissait pourtant d'un acte purement symbolique. En effet, la première réunion de cette commission ne devait avoir lieu qu'en mai 1912. Juste avant, le sous-secrétaire d'Etat chargé des travaux publics, des Postes et télégraphes, Charles Chaumet, empêcha le ministre de la Guerre, Adolphe Messimy, d'implanter tout autour de la terre des postes de télégraphie sans fil ; alors que le second ne songeait qu'à concurrencer l'hégémonie des liaisons sous-marines britanniques, le premier entendait protéger le réseau de câble français⁶... D'importantes avancées eurent tout de même lieu dans les deux années précédant le conflit mondial, notamment en ce qui concernait le recrutement et la formation des membres du comité de déchiffrement pour le temps de guerre.

L'alliance franco-russe devait permettre la troisième initiative. En 1906, il avait été décidé de créer une liaison radiotélégraphique directe entre les états-majors des

janvier 1914 [*Ibid.*, 5 N 7] et la nouvelle « note secrète sur l'organisation de la correspondance chiffrée dans l'armée » du 11 mars 1914.

¹ En 1903, le directeur de l'Ecole de télégraphie militaire du Mont-Valérien, le capitaine Gustave Ferrié, en installait un dans une baraque en bois aux pieds de la Tour Eiffel, tandis que les antennes réceptrices étaient placées au sommet ; en 1909, le poste était transféré dans un sous-sol des Invalides. S'en ajoutèrent ensuite dans les places de l'Est (Belfort, Epinal, Toul, Verdun, Maubeuge). Ferrié poussa ses études jusqu'à installer des postes dans des dirigeables et songea à équiper des avions [SHD/DAT, 7 N 1971, note de la 4^e direction du Génie du 19 octobre 1911].

² *Ibid.*, 9 Yd 778, il était entré en fonction le 15 février 1908 ; il resta à ce poste cinq ans, puis prit la direction du Deuxième bureau.

³ *Ibid.*, 1 K T 526, Mémoire du général Dupont.

⁴ Pour l'heure des systèmes des marines anglaise, italienne et espagnole. En 1904, ce fut au tour du système allemand de campagne d'être reconstitué. Pour s'entraîner, quelques télégrammes chiffrés de la guerre 1870-1871 furent également déchiffrés.

⁵ Cf. l'instruction interministérielle du 24 février 1906 [SHD/DAT, 16 N 1483].

⁶ De retour à la Guerre en juin 1914, il parvint à imposer un Réseau intercolonial, mais les hostilités avec les puissances centrales empêcha sa mise en œuvre. De même, pour lutter contre les brouillages ennemis, il doubla l'émetteur de la Tour Eiffel par deux postes à grande puissance à Lyon et Bucarest [Adolphe Messimy, *Mes souvenirs* (Paris, Plon, 1937), pp. 42-47].

armées française et russe pour le temps de guerre, dans le cadre de l'Alliance franco-russe. Après de multiples retards, les premières communications furent réalisées en août 1910 et le réseau fut ensuite complété pour compter, en juin 1914, trois lignes opérationnelles et une de secours. La question de la sécurité des échanges se posait cruellement puisqu'ils risquaient à tout moment d'être interceptés par l'Allemagne¹ et surtout son allié autrichien². Une série de protocoles furent donc signés entre les deux alliés ; le sixième, en mai 1911³, prévoyait la création d'un bureau central de TSF à Paris⁴ et à Saint-Pétersbourg. La création d'une section du Chiffre au ministère de la Guerre s'imposait. Créée officieusement le 22 février 1906, elle le fut officiellement le 22 juillet 1912.

Les décisions politiques avaient été particulièrement rapides. L'action du commandant Givierge avait été décisive. Profitant de sa nomination dans l'état-major particulier du nouveau ministre de la Guerre, Alexandre Millerand, il avait insisté sur les conséquences que ne manqueraient d'avoir l'inexistence d'une telle section comme le manque de formation des officiers affectés au chiffrement/déchiffrement dans les états-majors. Chargé d'étudier la création d'une section permanente du chiffre, il s'était tourné vers le commandant Cartier et avait été en mesure de proposer un projet dès le 20 juillet 1912 ; le 1^{er} septembre suivant, elle était opérationnelle. Rattaché au cabinet du ministre, l'effectif de la nouvelle section du chiffre se limitait à trois personnes : Cartier en prenait la direction, à la demande de Givierge, qui devenait son adjoint, auxquels s'ajoutait un administrateur civil ; trois personnels supplémentaires rejoindraient à la mobilisation. Ils s'occupaient du chiffrement et du déchiffrement de la correspondance du ministre, élaboraient, géraient et distribuaient les dictionnaires de chiffrement ainsi que les directives d'organisation et au fonctionnement du service de la correspondance chiffrée dans l'armée⁵. Enfin, elle prenait en charge le bureau central de TSF⁶. Le 12 janvier 1914, la commission de cryptographie militaire et le bureau militaire de déchiffrement fusionnaient avec la section du chiffre⁷. Le seul aléa contre lequel la section du Chiffre ne put lutter était le temps : le 30 juillet, redevenu ministre, Messimy déplorait qu'« il fallait plusieurs heures pour chiffrer, transmettre et déchiffrer un télégramme ».⁸

¹ L'Allemagne ne sembla pas se préoccuper d'interceptions radiotélégraphiques jusque dans les premiers mois de 1914 [Markus Pöhlmann, *op. cit.*].

² L'Autriche ne développa de *Dechiffrierdienst* qu'en novembre 1911, sous l'impulsion d'Andreas Fingl [Kriegsarchiv (KA) Vienna, Nachlass Ronge, B-58, Memorandum vom FML der Reserve August von Urbanski, octobre 1924.]. Cf. aussi John R Schindler, « A hopeless struggle: Austro-Hungarian cryptology during World War I », *Cryptologia*, octobre 2000.

³ SHD/DAT, 7 N 1940, Protocole n° 6 du 4 octobre 1911 entre la France et la Russie.

⁴ Le 14 novembre 1911, sa direction fut confiée au sous-chef de cabinet du ministre, auquel était adjoint le commandant Cartier [*Ibid.*, Annexe au protocole n° 6 du 4 octobre 1911 entre la France et la Russie].

⁵ Cf. les correspondances à destination des gouverneurs militaires et commandants des corps d'armée pour organiser les entraînements au « système cryptographique intégral » [*Ibid.*, 5 N 7, lettre du 11 juillet 1913].

⁶ Il pilotait l'activité de huit stations d'écoute, réparties sur le territoire national, dirigée vers les émetteurs allemands. Au commencement de la guerre, les procédures courantes et l'organisation du réseau ennemi étaient parfaitement connues du renseignement français. Il n'avait manqué au commandant Cartier que des radiogoniomètres pour positionner précisément sur une carte les émetteurs écoutés sans protections. Par le service de Renseignements, au début de 1914, il obtint l'Instruction officielle sur l'utilisation de la cryptographie dans l'armée allemande de juin 1913 [Olivier Lahaie, *op. cit.*, p. 1868 n. 138 et 1870, Markus Pöhlmann, *op. cit.*].

⁷ *Ibid.*, 5 N 7, Note (...) relative aux attributions de la section du Chiffre.

⁸ Adolphe Messimy, *op. cit.*, p. 169.

*

L'émergence de la cryptographie militaire en France et son développement rapide répondait plus à un souci d'adaptation à l'évolution technologique — notamment à l'usage du télégraphe lors des guerres de Sécession et franco-allemande de 1870-1871 — qu'à une innovation du renseignement. L'état-major général de l'Armée se préoccupait avant tout de la protection de ses communications, témoignant en cela une compréhension similaire à celle de la section de Statistique lorsque, à l'issue des années 1880, elle délaisse le renseignement pour se focaliser sur le contre-renseignement. Aussi bien la commission de télégraphie militaire que celle de cryptographie surestimèrent les capacités d'une Allemagne perçue comme omnisciente pour justifier leurs efforts. Les travaux du commandant Cartier à la section de Renseignements montraient bien que son objectif principal était de procurer des cryptogrammes au bureau de Déchiffrement plutôt que de développer des capacités d'interception.

Néanmoins, cet activisme amena la cryptographie militaire française à un niveau proche de bureau du Chiffre des Affaires étrangères, avec lequel la section de Renseignements était coupée suite à l'Affaire Dreyfus. Sur le plan international, elle dépassait les capacités allemandes et concurrençait celles de son alliée britannique ; seules la Russie¹ et l'Autriche la dominaient nettement. La Première Guerre mondiale constitua une phase d'évolution complémentaire. De la protection des communications, elle poussa la section du Chiffre du ministère de la Guerre à passer à l'offensive. Dès la mobilisation, elle entreprit de brouiller les échanges radio de l'ambassadeur allemand, Wilhelm von Schoen². Lisant les communications de l'ennemi, elle alimenta la section des Renseignements, mais elle ne parvint pas à se hisser au niveau des interceptions britanniques de la Room 40, qui décrypta le télégramme Zimmerman, le 16 janvier 1917...

Gérald Arboit
Juillet 2008

¹ Les Russes se montraient cependant d'une négligence en matière de sécurité des communications proches de celle des Allemands...

² Jean-Baptiste Duroselle, *Histoire de la Grande Guerre. La France et les Français, 1914-1920* (Paris, Richelieu, 1972), p. 64.