

Alexandre OLLIER



**LA
CRYPTOGRAPHIE
MILITAIRE**
avant la guerre de 1914

LAVAUZELLE

IST 2855

LA
CRYPTOGRAPHIE MILITAIRE
avant la guerre de 1914



Le Code de la propriété intellectuelle n'autorisant, aux termes des alinéas 2 et 3 de l'article L. 122-5, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » (alinéa 1^{er} de l'article L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et L. 335-3 du Code de la propriété intellectuelle.

© Copyright CHARLES LAVAUZELLE 2002

TABLE DES MATIÈRES

PRÉFACE	5
INTRODUCTION	7
CHAPITRE I. LE RENOUVEAU CRYPTOGRAPHIQUE EN FRANCE À LA FIN DU XIX^e SIÈCLE	17
1. LES CONDITIONS DU RENOUVEAU CRYPTOGRAPHIQUE	17
1.1. L'héritage de la guerre 1870-1871	17
1.1.1. <i>Le poids de la défaite</i>	17
1.1.2. <i>Une nouvelle organisation militaire : la conscription</i>	21
1.1.3. <i>Un pionnier en matière de cryptographie : le général Lewal</i>	22
1.2. Une révolution technique : l'invention du télégraphe électrique	27
1.2.1. <i>Télégraphie et cryptographie</i>	27
1.2.2. <i>La télégraphie militaire française</i>	32
1.3. Les travaux cryptographiques de nombreux militaires et civils	33
1.3.1. <i>Un pionnier : Auguste Kerckhoffs</i>	33
1.3.2. <i>Le commandant Bazeries</i>	37
1.3.3. <i>Une importante publication d'études cryptographiques</i>	40
1.3.3.1. Les travaux du marquis de Viaris.....	40
1.3.3.2. Les travaux du capitaine Valério.....	41
1.3.3.3. Quelques remarques sur les autres publications.....	43
	219

2. LA CRYPTOGRAPHIE DEVIENT UNE TECHNIQUE À PART ENTIÈRE	45
2.1. Le chiffrement et le déchiffrement	45
2.1.1. <i>Les méthodes de transposition</i>	45
2.1.1.1. Principes de fonctionnement.....	46
2.1.1.2. Un exemple historique de transposition double : le cryptographe 1886	47
2.1.2. <i>Les méthodes de substitution ou interversion</i>	49
2.1.2.1. La substitution à simple clef.....	49
2.1.2.2. La substitution à double clef.....	50
2.1.3. <i>Les méthodes à répertoire ou dictionnaire</i>	53
2.2. Le décryptement	56
3. LA SITUATION DE LA CRYPTOGRAPHIE MILITAIRE	62
3.1. Une cryptographie archaïque	62
3.1.1. <i>Une utilisation limitée de la cryptographie dans l'armée..</i>	62
3.1.2. <i>L'absence de spécialistes</i>	66
3.1.3. <i>Le rôle mineur de la télégraphie dans les communications militaires</i>	68
3.2. La prise de conscience de la faiblesse du Chiffre militaire français	70
3.2.1. <i>Le combat de Bazeries pour une réforme du Chiffre militaire : 1889-1901</i>	70
3.2.2. <i>La création d'une commission de cryptographie militaire.</i>	74
CHAPITRE II. LA CRYPTOGRAPHIE DEVIENT UN ÉLÉ- MENT DU RENSEIGNEMENT MILITAIRE AU DÉBUT DU XX^e SIÈCLE	81
1. L'ESSOR DE LA RADIOTÉLÉGRAPHIE ET SON UTI- LISATION MILITAIRE.....	81
1.1. L'invention de la TSF et ses enjeux	81

1.2. La radiotélégraphie militaire	86
1.2.1. <i>Les négociations pour l'acquisition de postes de radiotélégraphie</i>	86
1.2.2. <i>La recherche militaire en matière de radiotélégraphie</i>	89
1.3. Les liaisons radiotélégraphiques franco-russes	92
1.3.1. <i>Le rapprochement franco-russe</i>	92
1.3.2. <i>La création de liaisons radiotélégraphiques</i>	94
1.3.3. <i>Le fonctionnement des communications par TSF franco-russes.</i>	99
1.3.4. <i>La sécurité de ces liaisons radiotélégraphiques</i>	102
1.3.4.1. <i>Une solution provisoire insuffisante</i>	102
1.3.4.2. <i>Une organisation rationnelle de la correspondance chiffrée.</i>	104
2. UNE ÈRE DE COLLABORATIONS INTERMINISTÉRIELLES	106
2.1. Un rapprochement des ministères de l'Intérieur et de la Guerre	106
2.1.1. <i>Conséquences de l'affaire Dreyfus</i>	106
2.1.2. <i>La rivalité entre les Affaires étrangères et l'Intérieur au sujet de questions de cryptographie</i>	108
2.1.2.1. <i>Une collaboration efficace qui se termine mal</i>	108
2.1.2.2. <i>La création d'un service cryptographique à la Sûreté générale</i>	111
2.1.3. <i>La participation du capitaine Givierge aux travaux cryptographiques de la Sûreté</i>	113
2.2. La création d'une commission interministérielle de cryptographie	117
2.2.1. <i>Le problème de la surveillance de la correspondance télégraphique privée</i>	117
2.2.2. <i>L'émergence de cette commission en 1909</i>	122
2.2.3. <i>Des résultats mitigés</i>	123
	221

3. DES STRUCTURES INADAPTÉES - LA NÉCESSITÉ D'UN ORGANISME MILITAIRE PERMANENT ET SPÉCIALISÉ.....	125
3.1. La correspondance chiffrée dans l'armée.....	125
3.1.1. Une organisation rationnelle.....	125
3.1.2. Un système complexe.....	130
3.2. La commission de cryptographie militaire entre 1900 et 1912.....	133
3.2.1. La création d'un bureau de déchiffrement pour le temps de guerre.....	133
3.2.2. Les difficultés rencontrées par la commission de cryptographie militaire.....	135
3.2.3. De nombreux travaux réalisés	137
3.2.3.1. Les premières écoutes.....	138
3.2.3.2. La rédaction de notes techniques.....	139
3.2.3.3. Une tentative de centralisation.....	141
3.2.3.4. La mise au point de nouveaux procédés de chiffrement.....	141
3.2.3.5. Bilan des réalisations de la commission.....	143
CHAPITRE III. LA MISE EN PLACE D'UNE ORGANISATION RATIONNELLE ET CENTRALISÉE.....	145
1. LA CRÉATION DE LA SECTION DU CHIFFRE AU MINISTÈRE DE LA GUERRE EN 1912.....	145
1.1. Des circonstances favorables	145
1.1.1. L'affectation du capitaine Givierge à l'état-major particulier du ministre	146
1.1.2. L'importance des liaisons radiotélégraphiques franco-russes.....	147
1.2. L'intervention du capitaine Givierge.....	148
1.2.1. Première approche.....	148
1.2.2. L'assentiment du ministre de la Guerre	150
1.2.3. Bilan du rôle du capitaine Givierge.....	152

1.3. La difficile reconnaissance de la section du chiffre	154
1.3.1. <i>Les obstacles à son bon fonctionnement</i>	154
1.3.2. <i>Le renversement de situation</i>	157
1.3.3. <i>Récapitulatif des différents organismes liés au chiffre</i>	158
2. LA CENTRALISATION DE LA CRYPTOGRAPHIE MILITAIRE	159
2.1. La commission de cryptographie militaire de 1912 à 1914.	159
2.1.1. <i>Les difficultés de la commission</i>	159
2.1.2. <i>Le ralentissement des activités de la commission</i>	161
2.1.3. <i>Les insuffisances du bureau militaire de déchiffrement</i>	161
2.2. Les travaux de la commission interministérielle de cryptographie	163
2.3. Les travaux de la section du chiffre	164
2.3.1. <i>Une équipe efficace</i>	165
2.3.2. <i>La note secrète du 29 novembre 1912</i>	167
2.3.3. <i>L'organisation d'exercices réguliers sur le système SD</i>	169
2.3.4. <i>Des conférences sur la cryptographie</i>	172
2.3.5. <i>Les travaux du commandant Cartier</i>	173
2.3.5.1. <i>Sa participation à des commissions interministérielles..</i>	173
2.3.5.2. <i>La sécurité des communications par TSF de l'Aéronautique</i>	174
2.3.5.3. <i>La mise en place des services spéciaux de TSF</i>	176
2.3.6. <i>Les activités du capitaine Givierge</i>	177
2.3.7. <i>Les autres réalisations</i>	181
2.3.8. <i>La centralisation des questions de cryptographie</i>	182
3. LA CRYPTOGRAPHIE MILITAIRE AU DÉBUT DE LA GUERRE	183
3.1. La supériorité française	183
3.1.1. <i>La correspondance chiffrée</i>	183

3.1.2. <i>L'absence d'un organisme spécialisé allemand</i>	185
3.1.3. <i>Les carences de l'organisation française</i>	187
3.2. Une organisation du temps de guerre insuffisante	189
3.2.1. <i>La période précédant la mobilisation</i>	189
3.2.2. <i>Le service du chiffre aux armées</i>	192
3.2.2.1. Le départ du commandant Givierge au GQG.....	192
3.2.2.2. La création d'une section du chiffre au GQG.....	193
3.2.2.3. La création d'un service de chiffrement au niveau de chaque QG d'armée.....	194
3.2.2.4. Les dissensions au GQG.....	196
3.2.3. <i>La section du chiffre du ministère de la Guerre</i>	199
CONCLUSION	203
BIBLIOGRAPHIE	209
PRÉSENTATION DE LA COLLECTION	213
COMITÉ SCIENTIFIQUE	215
DANS LA COLLECTION	217
TABLE DES MATIÈRES	219



LAUZELLE

b.p. n° 8
87350 panazol

ISBN n° 2-7025-0535-X
Dépôt légal : Décembre 2002