CHIFFRE À L'APPUI
Avec l'avènement de la TSF, la question de la sécurité des messages, faciles à intercepter, se pose. Des codes secrets sont élaborés, que les services de cryptographie rivaux tentent de percer.
• *Centre d'écoutes français, Aisne.*

HULTON ARCHIVE/GETTY IMAGES

LE BOOM DES EXPERTS DU DÉCRYPTAGE

Jusqu'au début du XX^e^ siècle, les communications internationales passent par le câble du télégraphe et sont donc difficiles à intercepter. La TSF, mise en place juste avant la guerre, vient bouleverser la donne : les émissions radio, qui peuvent être interceptées par n'importe qui, doivent être codées si l'on veut préserver le secret des messages. Chaque pays a son approche des écoutes radio et du décryptage.

Dès le début de la guerre, la marine britannique isole l'Allemagne du reste du monde en sectionnant ses câbles télégraphiques, enfouis au fond des mers ; ce qui oblige celle-ci à recourir aux messages radio. L'Allemagne compte des cryptographes de valeur, notamment ceux du renseignement naval, qui décryptent les transmissions radio des navires britanniques entre 1914 et 1918. Mais ce savoir-faire ne sera guère décisif contre la France, qui privilégie les communications télégraphiques, hors de portée de leurs ennemis. Parmi les services cryptographiques des puissances centrales, celui de l'armée austro-hongroise se distingue par son efficacité, qui lui vaut une belle réputation. L'armée allemande connaît tout de même quelques succès en captant le trafic radio des Russes pendant la bataille de Tannenberg, en août 1914, et pendant la campagne des lacs de Mazurie de février 1915.

Côté français, une commission interministérielle de cryptographie est formée en 1909, qui regroupe les ressources des ministères de la Guerre, de la Marine et de l'Intérieur. Deux ans plus tard, le général Joffre, qui vient d'être nommé chef de l'état-major, fait créer une section du chiffre, placée sous les ordres du commandant Cartier.

Ubchi, ABC, etc.

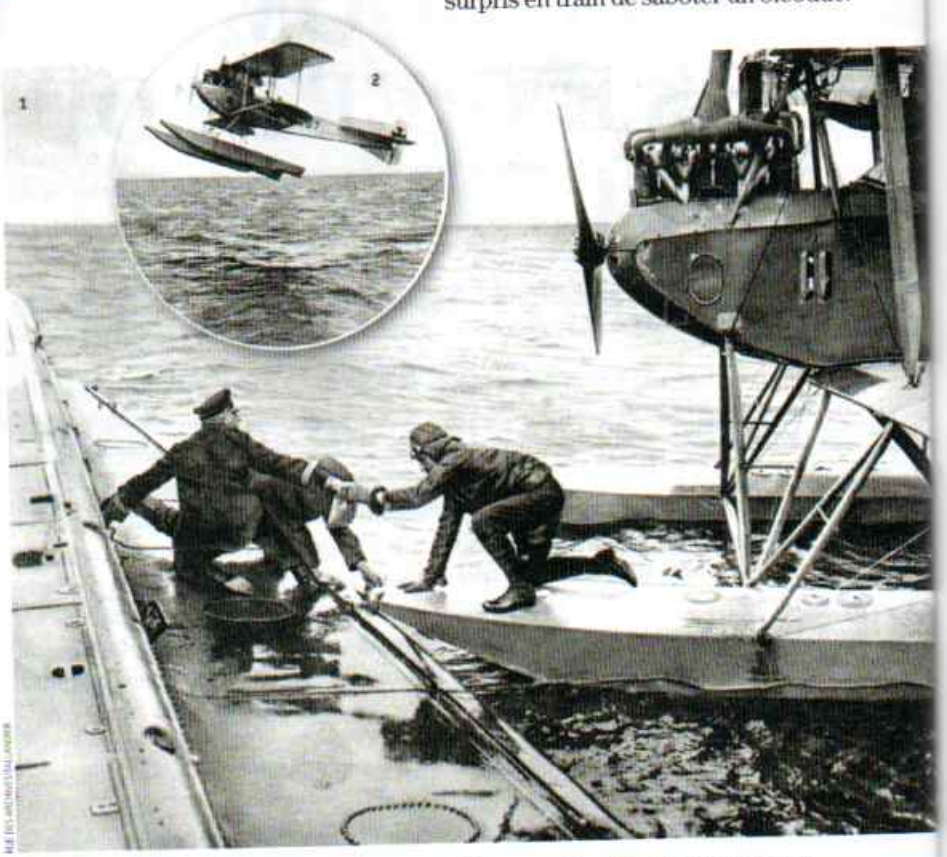
Polytechnicien, officier du génie, en poste au 2^e^ bureau de l'état-major de 1902 à 1912, Cartier est la cheville ouvrière de la commission interministérielle. Sa mission est d'abord de sécuriser les communications avec la Russie, probable alliée dans la guerre qui s'annonce mais séparée de la France par les Empires centraux. Dès 1914, les décrypteurs français maîtrisent le fonctionnement de l'Ubchi, la technique de codage des messages de »»

Chaque navire capturé ou coulé est désormais systématiquement fouillé, dans l'espoir de mettre la main sur les précieux carnets de codes et leurs clés

»» l'armée de terre allemande, vraisemblablement grâce à un officier allemand qui a vendu aux services français un manuel d'instruction en 1913.
À partir de novembre 1914, les belligérants s'enterrent dans les premières tranchées. Dès lors, le trafic radio diminue. Les Allemands commencent à se servir du réseau télégraphique en tirant des lignes jusqu'à leurs avant-postes. L'Ubchi est remplacé par un autre code, car ses utilisateurs ont compris qu'il était percé. La fuite vient d'un bulletin de renseignements britannique, tombé aux mains des Allemands via un officier fait prisonnier. C'est d'autant plus rageant que les Anglais prennent de haut les cryptographes français et rechignent à partager avec eux tous leurs secrets.

Du travail et des migraines

Les Français vont toutefois conquérir l'estime des Britanniques en leur envoyant, en janvier 1915, les clés du nouveau chiffre allemand, l'ABC. La même année, ils interceptent des messages clandestins envoyés d'Angleterre aux Pays-Bas, qui décrivent les mouvements de navires de la Royal Navy. Cette information, communiquée à Londres, permettra de démanteler un réseau allemand installé outre-Manche. De l'autre côté de la Manche, justement, on utilise parfois des procédés plus anciens : le MO5 (futur MI5, service de sécurité intérieure) démantèle au début du conflit un vaste réseau d'espionnage allemand en terre britannique grâce à une mesure toute simple, la censure postale : l'ouverture du courrier avait été autorisée en 1912 par Winston Churchill, alors ministre de l'Intérieur. Un petit groupe de cryptographes de la Royal Navy, installé dans un vieux bâtiment de l'Amirauté, à Whitehall, à Londres, est placé sous les ordres de l'amiral Reginald Hall. Avec les équipes des postes d'écoute radio déployées dans tout le royaume par l'Amirauté, elle va jouer un rôle central dans la défaite de l'Allemagne en interceptant très vite un grand nombre de messages codés.
Pour percer à jour un code, il faut beaucoup de travail – et autant de migraines –, ou de la chance. Le 20 août 1914, le corps sans vie d'un marin allemand est ramené par la mer sur la côte russe du golfe de Finlande. L'homme était opérateur radio sur un croiseur coulé par l'armée impériale de Nicolas II. On trouve sur lui un carnet sur lequel est inscrite la clé du code naval allemand. Comme elle ne sait pas l'exploiter, la marine russe le confie à son homologue britannique.
Second coup de chance : en décembre 1914, un chalutier britannique en mer du Nord attrape dans ses filets un autre carnet de codes. Voilà qui met le pied à l'étrier aux services de l'amiral Hall. Certes, les codes allemands diffèrent d'une armée à l'autre et sont régulièrement changés. Mais rien de tel pour comprendre la logique des codes ennemis. Désormais, tous les espions de Sa Majesté sont sensibilisés à l'importance de ces fameux carnets. Chaque navire ennemi capturé ou coulé est donc systématiquement fouillé. On récupère même un troisième carnet en Perse : le vice-consul allemand a été surpris en train de saboter un oléoduc.



BONNE PÊCHE En déchiffrant les signaux de l'Amirauté, les sous-marins allemands suivent à la trace les dragueurs de mines anglais. Ici, en 1917, le capitaine d'un U-boot remet des documents pris à l'ennemi.

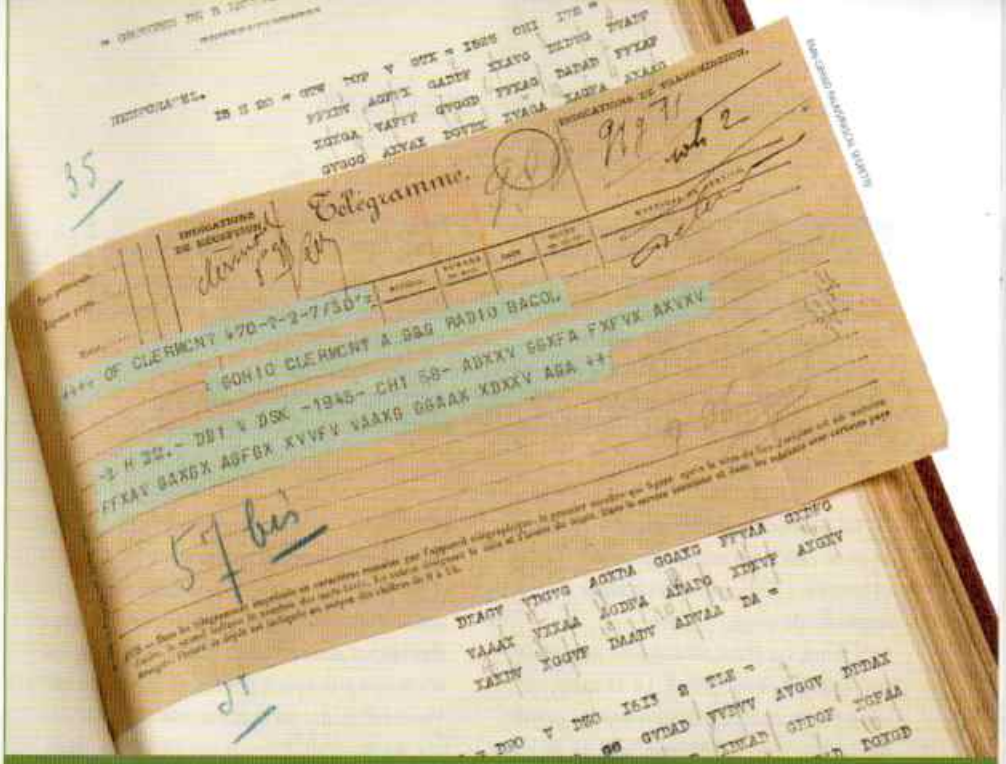
Il s'enfuit en abandonnant ses bagages. Dont l'un d'eux contient le précieux document.

De son côté, l'Allemagne se met en chasse des carnets de codes britanniques… et finit par en trouver. Cela lui permet notamment de suivre les signaux des dragueurs de mines britanniques. Ces derniers sont chargés de dégager des passages parmi les champs d'engins explosifs semés par les U-Boot, les sous-marins allemands. Dûment informée du travail des dragueurs de mines, la marine allemande renvoie des sous-marins qui déposent de nouvelles mines. L'amiral Hall, qui a compris la manœuvre, fait annoncer le déminage – fictif – d'un couloir au large de Waterford, en Irlande. Un U-Boot arrive peu après et saute sur une de ses propres mines. Pourquoi Waterford ? Parce que l'endroit est peu profond. L'Amirauté peut y envoyer des hommes-grenouilles… qui récupèrent un carnet de codes tout neuf !

Des formules familières

Après ces débuts intensifs, le département de cryptographie de la Royal Navy, désormais familier des formules de salutations et mentions récurrentes, ne met guère que six à huit heures pour décoder un nouveau message radio, alors que la clé est modifiée chaque semaine. Ce travail contribue de manière sensible à maintenir la prédominance britannique sur les mers et limite l'impact meurtrier des U-boot, qui auront néanmoins fait des ravages sur le ravitaillement transatlantique : de septembre 1914 à décembre 1915, ils envoient par le fond 225 navires de commerce.

Pendant ce temps, en France, la section du chiffre se développe sensiblement, ses effectifs passant de 15 personnes en 1915 à 59 en 1916. Parmi les nouvelles recrues, un petit génie des codes va se révéler, Georges Painvin… ◆



LIGNES ENNEMIES **À l'issue d'une course contre la montre pour percer le code ADFGVX, le capitaine français prévient l'offensive allemande du 9 juin 1918, entre Montdidier et Noyon.** *• Carnet de travail de décryptement de Painvin, musée des Transmissions, Cesson-Sévigné.*

GEORGES PAINVIN, L'HOMME CLÉ DU CHIFFRE

« Le capitaine Georges Painvin, le plus grand expert en code qu'ait eu la France, génie analytique de premier ordre, avait une manière de résoudre les messages en code qui tenait de la sorcellerie. » Ce n'est pas un auteur cocardier qui le dit mais Herbert Yardley, ex-responsable du décryptage américain, dans son ouvrage *The American Black Chamber* (1931). Pourtant, Painvin est alors inconnu du public français et le restera.

Originaire de Nantes, d'allure juvénile, ce diplômé de Polytechnique et des Mines semble avoir tous les talents : 1er prix de violoncelle au conservatoire, professeur de chimie, géologie et paléontologie, administrateur de diverses sociétés après la guerre, réorganisateur de la Bourse de Paris, président d'Ugine, du Crédit commercial de France, et on en passe. Painvin arrive de la 6e armée, où il servait comme officier d'ordonnance. De sa propre initiative, il est parvenu à décrypter certains des télégrammes allemands, émis par TSF en morse, qui passaient entre ses mains. Painvin, qui s'est lié d'amitié avec le capitaine Paulier, chiffreur, s'initie sur le tas aux mystères du chiffre, où il est transféré.

Les Allemands changent souvent de code. En janvier 1916, l'ABC est remplacé par un code cousin, l'ABCD, déjà en service sur le front est. Le nouveau venu, Painvin, s'y attaque et le brise en à peine deux semaines, se taillant une réputation de petit prodige. Avril 1916 : nouveau changement et solution tout aussi rapide de celui qui devient l'homme clé du service. Cartier résume ainsi son rôle central : « La supériorité du capitaine Painvin s'affirmait nettement et c'est lui qui identifia pour tous les codes les 150 ou 200 groupes qui permettaient un commencement de décryptement partiel que les autres cryptologues étendaient rapidement. »

Après le traité de Brest-Litovsk, signé en mars 1918, l'Allemagne a enfin réussi à sortir du jeu la Russie et peut reporter ses forces sur le seul front de l'Ouest. Elle veut l'emporter rapidement, avant que ›››

Chaque navire capturé ou coulé est désormais systématiquement fouillé, dans l'espoir de mettre la main sur les précieux carnets de codes et leurs clés

»» l'armée de terre allemande, vraisemblablement grâce à un officier allemand qui a vendu aux services français un manuel d'instruction en 1913.
À partir de novembre 1914, les belligérants s'enterrent dans les premières tranchées. Dès lors, le trafic radio diminue. Les Allemands commencent à se servir du réseau télégraphique en tirant des lignes jusqu'à leurs avant-postes. L'Ubchi est remplacé par un autre code, car ses utilisateurs ont compris qu'il était percé. La fuite vient d'un bulletin de renseignements britannique, tombé aux mains des Allemands via un officier fait prisonnier. C'est d'autant plus rageant que les Anglais prennent de haut les cryptographes français et rechignent à partager avec eux tous leurs secrets.

Du travail et des migraines

Les Français vont toutefois conquérir l'estime des Britanniques en leur envoyant, en janvier 1915, les clés du nouveau chiffre allemand, l'ABC. La même année, ils interceptent des messages clandestins envoyés d'Angleterre aux Pays-Bas, qui décrivent les mouvements de navires de la Royal Navy. Cette information, communiquée à Londres, permettra de démanteler un réseau allemand installé outre-Manche. De l'autre côté de la Manche, justement, on utilise parfois des procédés plus anciens : le MO5 (futur MI5, service de sécurité intérieure) démantèle au début du conflit un vaste réseau d'espionnage allemand en terre britannique grâce à une mesure toute simple, la censure postale : l'ouverture du courrier avait été autorisée en 1912 par Winston Churchill, alors ministre de l'Intérieur. Un petit groupe de cryptographes de la Royal Navy, installé dans un vieux bâtiment de l'Amirauté, à Whitehall, à Londres, est placé sous les ordres de l'amiral Reginald Hall. Avec les équipes des postes d'écoute radio déployées dans tout le royaume par l'Amirauté, elle va jouer un rôle central dans la défaite de l'Allemagne en interceptant très vite un grand nombre de messages codés.
Pour percer à jour un code, il faut beaucoup de travail – et autant de migraines –, ou de la chance. Le 20 août 1914, le corps sans vie d'un marin allemand est ramené par la mer sur la côte russe du golfe de Finlande. L'homme était opérateur radio sur un croiseur coulé par l'armée impériale de Nicolas II. On trouve sur lui un carnet sur lequel est inscrite la clé du code naval allemand. Comme elle ne sait pas l'exploiter, la marine russe le confie à son homologue britannique.
Second coup de chance : en décembre 1914, un chalutier britannique en mer du Nord attrape dans ses filets un autre carnet de codes. Voilà qui met le pied à l'étrier aux services de l'amiral Hall. Certes, les codes allemands diffèrent d'une armée à l'autre et sont régulièrement changés. Mais rien de tel pour comprendre la logique des codes ennemis. Désormais, tous les espions de Sa Majesté sont sensibilisés à l'importance de ces fameux carnets. Chaque navire ennemi capturé ou coulé est donc systématiquement fouillé. On récupère même un troisième carnet en Perse : le vice-consul allemand a été surpris en train de saboter un oléoduc.

BONNE PÊCHE En déchiffrant les signaux de l'Amirauté, les sous-marins allemands suivent à la trace les dragueurs de mines anglais. Ici, en 1917, le capitaine d'un U-boot remet des documents pris à l'ennemi.

Secret défense oblige, les historiens ne prendront connaissance que cinquante ans après la guerre de l'activité de décryptement des services français

X-MAN Georges Painvin pose avec ses camarades de l'École polytechnique, dont il sortira 2e, en 1905.

ÉCOLE POLYTECHNIQUE

›››› les Américains ne montent en puissance, et pour cela prépare une grande offensive… l'occasion de changer à nouveau de code.

Le 5 mars, les Français captent le premier message en code ADFGX. Le 11 mars, ce code est complété par un nouveau carnet de chiffrement, le *Schlüsselheft*. Le 21 mars, alors que les Français ne peuvent plus lire aucun des messages ennemis, les Allemands lancent leur grande offensive. Ils font une percée entre Cambrai et Saint-Quentin. Mais, le 27 mars, on trouve sur un prisonnier allemand le *Schlüsselheft*. Avec quatre collègues, Painvin travaille jour et nuit pour exploiter cette trouvaille. Le 28 mai est lancée l'attaque allemande du Chemin des Dames. Trois jours plus tard, Painvin trouve la nouvelle clé. Toutefois, le 1er juin, tout est à recommencer : les Allemands changent encore leur code pour l'ADFGVX. Les soldats du général Ludendorff, alors à quelques dizaines de kilomètres de Paris, préparent une quatrième offensive qui se veut déterminante. Pourquoi une telle précaution ? Peut-être parce qu'un message capital est envoyé ce 1er juin 1918 par le QG allemand aux avant-postes de la région de Montdidier, qui ne doit surtout pas être lu par les Français. Painvin, surmené, n'arrive plus à travailler. Il est dans un tel état d'épuisement qu'il doit être hospitalisé. Mais il continue à chercher… Une gaffe (emploi d'une phrase stéréotypée) lui donne une ouverture. Le 3 juin, la réponse tombe : c'est à Montdidier qu'aura lieu le prochain assaut ! « Accélérer la montée des munitions. Même pendant le jour, partout où l'on n'est pas vu. » Ce message va être baptisé par les historiens le « Télégramme de la victoire ». Certes, ce succès allié n'emporte pas à lui seul la victoire finale, mais il marque un tournant dans le conflit. Les divisions du général Mangin sont concentrées là où se déclenche, le 9 juin, l'offensive allemande. Celle-ci échoue. La contre-offensive va devenir la bataille du Matz, que les Français remportent grâce à Painvin. Épuisé par ses efforts, celui-ci mettra des mois à récupérer. Il sera décoré après 1918 de la Légion d'honneur, de la *Military Cross* britannique et de la Croix de chevalier de la couronne d'Italie. Rendu à la vie civile, il observera pendant cinquante ans le plus grand silence sur ses activités pendant la guerre. ◆

Les Américains abusent du temps d'antenne

L'OREILLE EN CAMPAGNE Formés sur le tard, par les Français, à la cryptographie, les Américains s'empressent de combler leurs lacunes, jusqu'à espionner leurs alliés ! • *Une station radio mobile américaine.*

Les Américains entrent tardivement dans le conflit et ne disposent pas de service de cryptographie. Ce sont en grande partie les Français qui vont les aider à en bâtir un. Le colonel Cartier, patron du service du chiffre, leur enseigne les bases de la cryptographie. Au printemps 1918, on effectue un échange de personnel à des fins de formation. Les Américains lancent la mission Yardley, du nom d'un cryptographe dépêché auprès du service de renseignements de la Navy et du colonel Cartier pour obtenir le code allemand. Les deux refusent.

Les Américains sont jugés trop désinvoltes : à peine formés au décryptage, ils installent des antennes TSF à Paris et à Lyon sans autorisation. À l'approche de la fin de la guerre, les intérêts nationaux reprennent leurs droits. La suite leur donnera raison : pendant la négociation du traité de Versailles, Yardley installe un bureau du chiffre qui espionne tout le monde, y compris ses alliés ! Un travers qui ne fera que s'accentuer… ◆

La manne du télégramme Zimmermann

L'Histoire a surtout retenu le principal succès des décrypteurs anglais de Whitehall : le fameux télégramme Zimmermann, qui a déclenché l'entrée en guerre des États-Unis. Début 1917, ceux-ci restent fidèles – du moins en apparence – à leur politique de neutralité, malgré les dommages causés à leurs navires par les U-boot et les saboteurs allemands. Pour espérer l'emporter, l'Allemagne a absolument besoin de bloquer les ravitaillements américains vers l'Angleterre. Elle prévoit donc d'intensifier sa guerre sous-marine dans l'océan Atlantique. Dans le cas où les États-Unis entreraient en guerre, il serait nécessaire d'allumer un contre-feu pour fixer l'armée américaine. Quel autre allié possible en pareil cas que le Mexique, pays frontalier ? Du coup, le 16 janvier, le ministre allemand des Affaires étrangères, Arthur Zimmermann, adresse à son ambassadeur à Mexico une offre d'alliance à transmettre au président mexicain : « Nous proposons au Mexique une alliance dans les conditions suivantes : une aide financière généreuse et un engagement de notre part que le Mexique va reconquérir les territoires perdus au Texas, au Nouveau-Mexique et en Arizona. Vous informerez le président de cela le plus secrètement possible dès que le déclenchement de la guerre avec les États-Unis est certain. Veuillez attirer l'attention du président sur le fait que l'utilisation implacable de nos sous-marins offre désormais la perspective de contraindre l'Angleterre à faire la paix en l'espace de quelques mois. »

Oubliée, la non-belligérance

La manœuvre, qui n'est pas spécialement subtile, offre aux Britanniques une occasion en or. Encore faut-il qu'ils « blanchissent » le renseignement, c'est-à-dire qu'ils le transmettent aux Américains sans leur avouer qu'ils l'ont obtenu en les espionnant.

Une fois authentifié, le télégramme fait l'effet d'une bombe dans l'opinion américaine. Et il offre au président américain, Thomas Woodrow Wilson, qui avait fait campagne en vue de sa réélection sur le thème de la non-belligérance, un prétexte en béton pour faire le contraire de ce qu'il avait promis. ◆