La Revue de la BNU

13 | 2016
Varia 13

« Britain's best kept secret » : la machine Enigma et le décodage des messages durant la Seconde Guerre mondiale

Christian Westerhoff et Thomas Weis

Traducteur : Françoise Bornemann

OpenEdition Journals

Édition électronique
URL : http://journals.openedition.org/rbnu/1512
DOI : 10.4000/rbnu.1512
ISSN : 2679-6104

Éditeur
Bibliothèque nationale et universitaire de Strasbourg

Édition imprimée
Date de publication : 1 mai 2016
Pagination : 62-71
ISBN : 9782859230623
ISSN : 2109-2761

Référence électronique
Christian Westerhoff et Thomas Weis, « « Britain's best kept secret » : la machine Enigma et le décodage des messages durant la Seconde Guerre mondiale », *La Revue de la BNU* [En ligne], 13 | 2016, mis en ligne le 01 mars 2020, consulté le 11 décembre 2020. URL : http://journals.openedition.org/rbnu/1512 ; DOI : https://doi.org/10.4000/rbnu.1512

La Revue de la BNU est mise à disposition selon les termes de la Licence Creative Commons Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 4.0 International.

View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by OpenEdition

L'Enigma et ses cylindres permutables
(coll. Württembergische Landesbibliothek Stuttgart)

« BRITAIN'S BEST KEPT SECRET » :

la machine Enigma et le décodage des messages durant la Seconde Guerre mondiale

Un des plus grands mystères de la Seconde Guerre mondiale fut le décodage réussi des messages radio que les Allemands avaient cryptés grâce à la machine à coder « Enigma » (voir ill. ci-contre). Jürgen Rohwer, ancien directeur de la Bibliothèque d'histoire contemporaine (Bibliothek für Zeitgeschichte–BfZ), s'est livré à des recherches approfondies sur la question de savoir comment les Alliés étaient parvenus, au cours de la guerre, à empêcher les sous-marins allemands de torpiller les bâtiments anglais et américains dans l'Atlantique. Ces succès, ils les durent surtout à l'opération secrète nommée « Ultra » (de « ultra secret »), qui resta inconnue de tous durant des décennies. Le texte qui suit raconte l'histoire de ce décodage d'Enigma, l'importance de ce fait dans le déroulement de la Seconde Guerre mondiale, la révélation au public dans les années 70 de l'opération secrète « Ultra » et les travaux des historiens qui s'y rapportent.

La guerre dans l'Atlantique

La Grande-Bretagne était très dépendante, durant la Seconde Guerre mondiale, de son approvisionnement par voie maritime. Comme elle l'avait déjà fait au cours de la guerre précédente, la marine allemande essayait d'attaquer les navires qui faisaient route vers la Grande-Bretagne, pour ainsi lui couper les vivres. Comme la marine de guerre allemande était bien inférieure à son homologue anglaise, cela ne pouvait se faire qu'à l'aide de sous-marins. Pour sécuriser leurs convois, les Britanniques mirent en place des escortes. En nombre, les navires de transport traversaient l'Atlantique, accompagnés par des escorteurs qui les protégeaient des sous-marins ennemis. Les Allemands réagirent en envoyant des sous-marins à la rencontre de ces convois afin de les intercepter. La coordination entre les sous-marins se faisait par radio. Pour que ces opérations en mer réussissent, il était indispensable que les messages radio ne puissent pas être écoutés par l'ennemi.

L'Enigma : historique et mode de fonctionnement

Durant la Première Guerre mondiale, les Alliés avaient tiré d'importants avantages stratégiques de l'analyse qu'ils avaient faite des communications radio des Allemands. Face à ce qui, à la fin de la guerre, avait été reconnu comme une « catastrophe cryptographique », l'armée allemande avait cherché une méthode sûre pour coder ses messages radio. S'inspirant d'outils déjà utilisés, Arthur Scherbius élabora au début des années 20 un appareil de codage auquel il donna le nom grec d'Enigma. La marine allemande en acquit en 1926 une version spécialement modifiée à des fins militaires. Cet appareil, mis en œuvre par la Wehrmacht en 1935, fut utilisé avec quelques modifications jusqu'à la fin de la guerre en 1945. Enigma n'est ni une machine à écrire ni un poste émetteur. C'est un poste afficheur qui remplace chaque lettre d'un texte par une autre et fait donc de ce texte un message codé, qui est ensuite noté sur papier et transmis en morse. En sens inverse, l'appareil peut retraduire en langage clair un message codé. Enigma est principalement composé des pièces suivantes : 1) un clavier, 2) plusieurs cylindres rotatifs, 3) un cylindre

fixe pour le retour, 4) un panneau à fiches, 5) un espace d'affichage (voir ill. ci-contre). Les cylindres rotatifs sont au cœur du processus de codage. Lorsqu'on appuie sur une touche du clavier (par exemple sur le « S »), un courant électrique produit par une batterie parcourt les cylindres et c'est une autre lettre qui s'allume (voir ill. ci-contre : le « N ») ; celle-ci est la lettre codée. Lors du décodage, les lettres lumineuses redonnent le texte en clair.

Pour que codage et décodage se déroulent parfaitement, émetteur et récepteur doivent avoir initialement positionné les cylindres de la même manière. Il faut choisir 3 cylindres dans un ensemble de 5, ou même de 8, et les faire fonctionner selon un ordre mis au point avec le récepteur. Ensuite, les cylindres doivent être remis dans leur position initiale de manière coordonnée elle-même avec le récepteur. Sur ces cylindres sont gravés soit l'alphabet de 26 lettres, soit les chiffres arabes de 1 à 26 qui correspondent à la place des lettres dans l'alphabet. Chaque cylindre peut être tourné isolément et mis dans une position de départ déterminée, grâce à son cerclage extérieur.

Les fils électriques à l'intérieur des cylindres sont positionnés de façon différente pour chacun d'eux. Ce système de fils ne peut être modifié (voir ill. p. 65). Le signal électrique déclenché par le fait d'appuyer sur une touche du clavier est transmis de cylindre en cylindre par des interconnexions. Un cylindre, le cylindre de « retour » placé tout à gauche, ne tourne pas, mais convertit les lettres et transmet le signal aux cylindres rotatifs. Le signal effectue alors le chemin inverse. Par le système des fils à l'intérieur des cylindres, le chemin n'est cependant pas le même qu'à l'aller (voir ill. p. 66).

Tous les cylindres sont reliés les uns aux autres mécaniquement. Le premier cylindre tourne d'un contact à chaque fois qu'une touche est frappée. Lorsqu'il a effectué une rotation complète, le second cylindre tourne lui aussi d'un contact. Ce principe se reproduit avec le troisième cylindre. Le tableau qui se trouve à l'avant de l'appareil (voir ill. p. 66 en bas) sert à augmenter les possibilités de permutation de lettres. Grâce à ce système de câblage, certaines lettres peuvent être interverties, par exemple le « T » devient « U ».

Le risque de rendre les messages déchiffrables augmente avec la longueur de ceux-ci et si le mode de codage reste le même tout au long du texte. Pour cette raison, Enigma devait être reprogrammée le plus souvent possible et la longueur des messages devait être réduite à 250 signes. On reprogrammait en fait tous les jours la machine, et même plusieurs fois par jour.

Les points faibles du codage

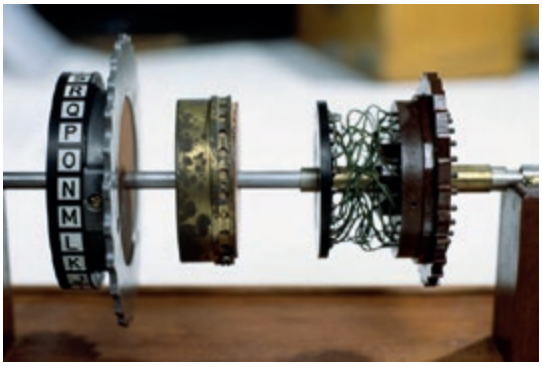
Les avantages d'Enigma sont dus avant tout aux cylindres et à leur système de rotation. Par le biais de cette dernière, on obtient que chaque lettre se trouve remplacée par une autre (codage polyalphabétique). Ainsi les tentatives classiques de déchiffrement des textes secrets, de même que les analyses statistiques ou les recherches de modèles, sont vouées à l'échec. Et cependant, plusieurs facteurs firent que dès le début de la guerre l'Enigma de la Wehrmacht n'offrit plus une sécurité suffisante. Une des raisons en fut ce qu'on appelle les « cribs » ou « mots probables ». On pouvait les relever dans les rapports militaires ou les bulletins météorologiques, qui arrivaient tous les matins à heure fixe, et étaient émis du même endroit. Leur contenu était souvent très stéréotypé et truffé de « cribs », comme par exemple MINENSPERRE (barrage de mines) ou GELEITZUG (convoi escorté), mots que les casseurs de codes britanniques utilisèrent pour le décryptage. Il arrivait aux Anglais de provoquer eux-mêmes des événements afin de recevoir des messages au contenu qu'ils pouvaient présupposer.

Le décodage : les services secrets polonais

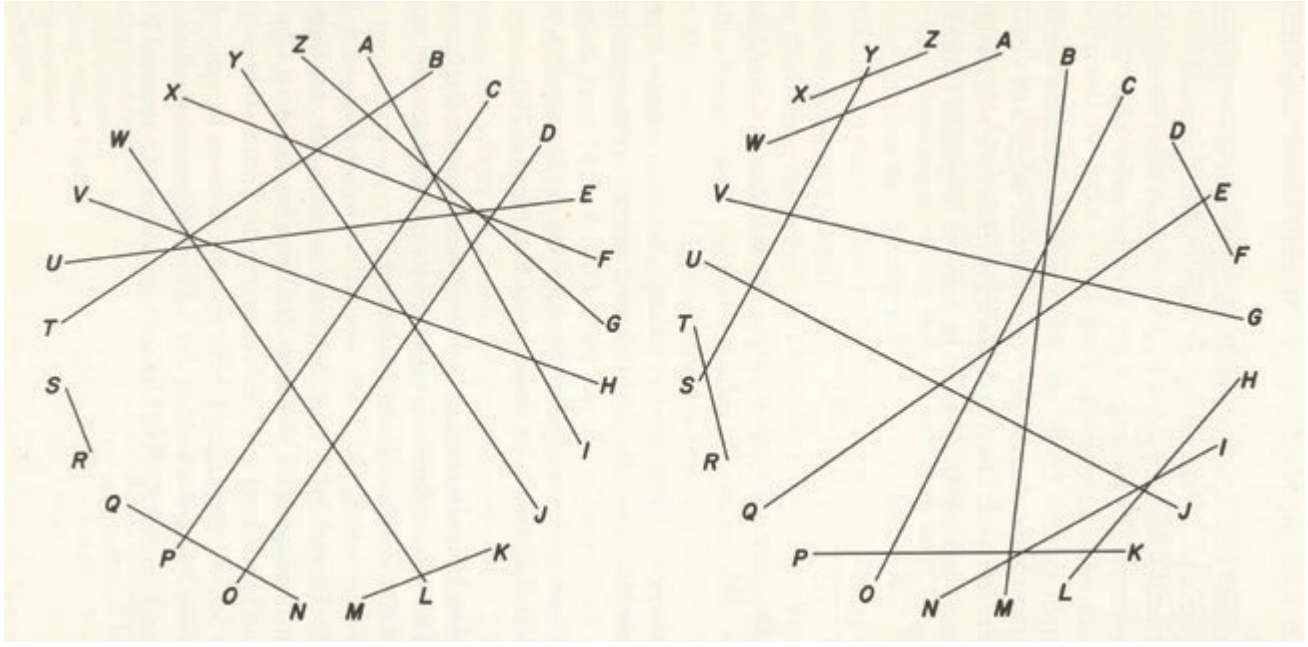
Très vite, il y eut des tentatives visant à déverrouiller Enigma. Dans les années 20, les services secrets polonais réussirent à acquérir quelques appareils Enigma proposés en version civile dans le commerce. La version militaire était beaucoup utilisée en Prusse occidentale lors des manœuvres allemandes. De nombreux messages codés furent interceptés par les Polonais, ce qui leur permit de comprendre l'utilisation des cylindres à l'intérieur des appareils militaires et la façon dont fonctionnait leur système de câblage électrique interne. Les Polonais réussirent même à fabriquer une copie de la version militaire d'Enigma.

En 1932, Hans-Thilo Schmidt, un espion d'origine allemande travaillant pour la France sous le nom de HE (Asché), remit au futur général Gustave Bertrand, alors membre des services secrets français, des tableaux de codage ainsi qu'un mode d'emploi et d'autres documents relatifs aux codages d'Enigma. Le deuxième bureau des services secrets français transmit ces documents aux services anglais et polonais. Alors que Français et Anglais ne parvenaient pas à comprendre les mécanismes du codage, le mathématicien polonais Marian Rejevski, alors âgé de 27 ans, réussit en 1932 une première intrusion dans Enigma.

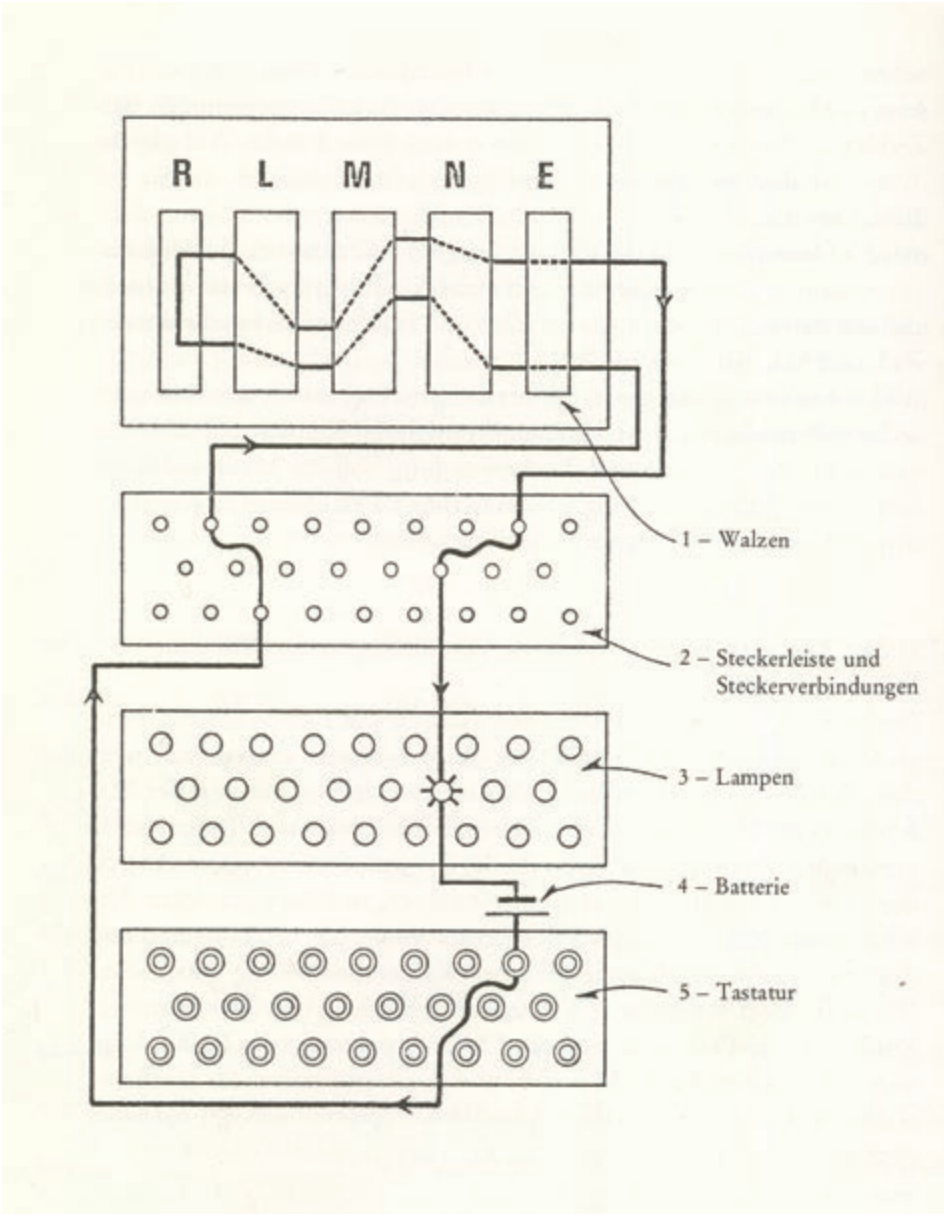
Le clavier et l'espace d'affichage



Les câblages internes des cylindres



Graphique des câblages internes
(coll. Württembergische Landesbibliothek Stuttgart)



Trajet du signal électrique par le tableau et par les cylindres
(coll. Württembergische Landesbibliothek Stuttgart)

Le tableau (panneau à fiches)

À la veille de la Seconde Guerre mondiale, les Polonais livrèrent leur savoir aux Britanniques et aux Français ébahis. Les 26 et 27 juillet 1939, lors d'une rencontre secrète dans la forêt de Pyry, à 20 km au sud-est de Varsovie, les casseurs de codes polonais présentèrent au major Bertrand, au cryptologue français Henri Braquenié ainsi qu'à des membres des services secrets britanniques leur copie d'Enigma ainsi que des appareils de cryptanalyse développés par leurs soins.

Les Anglais et les Américains

Suite à l'invasion de la Pologne par les Allemands, le centre de décodage de la forêt de Pyry dut être abandonné. Cependant les cryptologues polonais réussirent à échapper à la Wehrmacht et à l'Armée rouge. D'éminents experts purent passer en France via la Roumanie et vinrent aider les Français de la « section Z » dans leur centre de décodage de Vignolles, près de Paris. Lorsque les troupes allemandes marchèrent sur la capitale française en 1940, il fallut aussi vider sans délai les lieux à Vignolles. Les machines Enigma qui s'y trouvaient, ainsi que les documents et autres archives, furent détruits ; Bertrand et son équipe purent gagner l'Algérie en avion. Désormais les Anglais devaient faire face tout seuls. Les cryptanalystes britanniques se mirent au travail du décodage d'Enigma à Bletchley Park, à 70 km au nord-est de Londres. Jusqu'à 14 000 femmes et hommes furent mobilisés pour intercepter et décoder les messages radio allemands.

Le temps mis à trouver la clé des codes du jour était de première importance. Le grand mathématicien Alan Turing fut d'avis que ce temps ne pouvait être réduit qu'à l'aide d'une machine. En toute hâte, il poussa à la construction d'un calculateur analogique. Son idée était de réduire de façon drastique le nombre des combinaisons de codage, qui pouvait dépasser les 200 trilliards (200 000 trillions), en reliant en un système circulaire plusieurs ensembles de cylindres du modèle Enigma. Les combinaisons restantes passaient par la « bombe Turing » et on finissait par trouver la position correcte de décodage.

Alors que dès le 22 mai 1940, on réussit à rentrer dans les communications radio de l'aviation, le décodage de la radio marine se fit attendre. L'appareil Enigma utilisé par la marine avait des cylindres interchangeables dont les câblages électriques étaient inconnus des Anglais. Le 9 mai 1941, le destroyer anglais HMS Bulldog captura le sous-marin allemand U-110 et put s'emparer d'une machine Enigma de marine intacte, ainsi que de tous les documents secrets concernant son utilisation. De la sorte, les Anglais furent en mesure au cours de ce même mois de décoder les communications allemandes. Mais ce succès fut de courte durée. En 1942, la marine allemande introduisit une Enigma à quatre cylindres (« M4 »), avec de nouveaux cylindres interchangeables. Pendant toute une année, les cryptologues de Bletchley Park se retrouvèrent « aveugles ».

Après l'entrée en guerre des États-Unis, Anglais et Américains mirent en commun leurs succès en décodage. Les Américains purent ainsi améliorer la « bombe Turing ». À partir d'avril furent fabriqués plus de 120 exemplaires d'une variante ultra-rapide spécialement conçue pour s'attaquer à la M4. Dorénavant, c'en était fait de la sécurité des sous-marins allemands, et ce fut le cas jusqu'à la fin de la guerre.

Négligences allemandes

Du côté allemand, on était en général si convaincu de l'inviolabilité d'Enigma qu'on n'imaginait même pas qu'une intrusion ennemie y fût possible. Comme les informations militaires perdent très vite leur actualité en temps de guerre, on pensait aussi qu'un éventuel décodage prendrait trop de temps pour en tirer une quelconque efficacité. Par conséquent, on ne chercha guère à améliorer l'appareil. Pourtant on remit en cause durant la guerre la sécurité du codage d'Enigma, notamment l'amiral Dönitz qui commandait la flotte des sous-marins. Peu après l'entrée des troupes allemandes en Pologne déjà, on prit note des succès de la section polonaise de décodage et de sa reconstitution de cylindres Enigma. En outre, le haut commandement de la Wehrmacht reçut en 1943, de la part du service de renseignements de la Suisse, une note au sujet des « casseurs de code » de Bletchley Park. Le service de renseignements de la marine contrôla donc à plusieurs reprises la sécurisation d'Enigma, mais ne le fit que sur des bases théoriques et en se fondant sur des constatations statistiques. C'est seulement à partir de janvier 1944 qu'un expert du service de renseignements de la marine « cassa » de façon empirique l'appareil Enigma et présenta en juin 1944 une liste des principales erreurs commises dans son utilisation. Mais à ce moment-là, il était déjà trop tard pour les améliorations.

Conséquences du décodage

La fragilisation d'Enigma fut d'une importance capitale, tant stratégique que tactique, dans la poursuite de la Seconde Guerre mondiale. Beaucoup d'historiens pensent que le décodage d'Enigma n'a pas changé le cours de la guerre, mais que celle-ci aurait sans doute duré plus longtemps et fait encore plus de victimes. Pour la bataille de l'Atlantique, le décodage du système radio allemand fut d'une importance capitale. Grâce à l'opération « Ultra », les attaques qu'eurent à subir les navires des escortes ne purent pas être complètement évitées, mais les convois menacés purent être renforcés de façon plus efficace par la connaissance des positions des sous-marins ennemis (voir ill. ci-contre). Grâce au décodage américain, on put torpiller en été 1943 des tankers sous-marins allemands (U-Tanker). Sans ces navires ravitailleurs, les sous-marins allemands ne pouvaient rester en mer et devaient se faire remorquer vers la France. La guerre sous-marine fut ainsi définitivement perdue pour les Allemands. Dans le succès du débarquement en Normandie également, l'opération « Ultra » joua un rôle important. Ainsi le code Enigma pour le D-Day, le jour du débarquement des Alliés en Normandie, fut décrypté en moins de deux heures à l'aide du crib « Wettervorhersage Biskaya » (prévision météo Biscaye) par les cryptanalystes anglais qui n'eurent aucun mal à le deviner et à voir leurs suppositions confirmées.

Un secret longtemps gardé

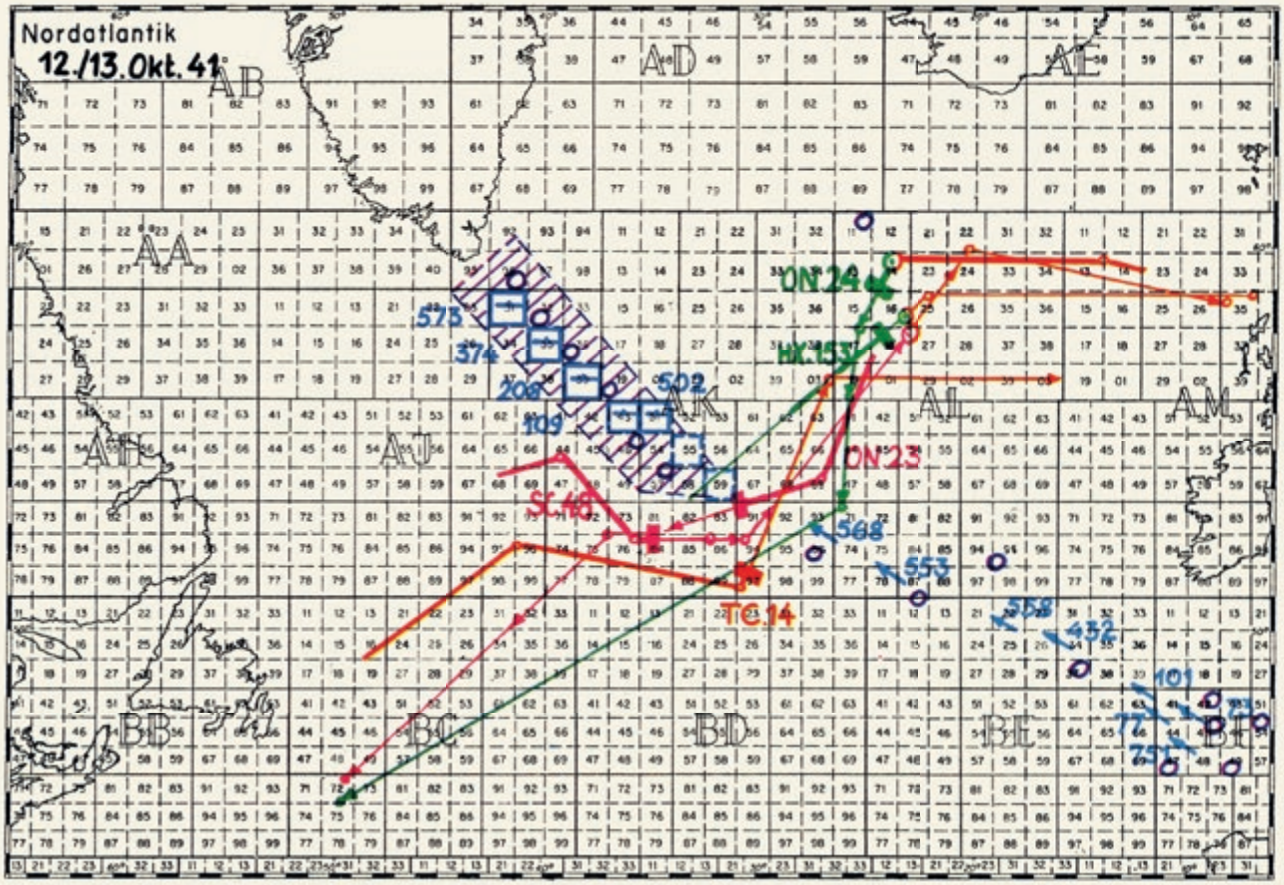
Ce savoir accumulé grâce à toutes les élucidations concernant la transmission radio, les Alliés ne le divulguèrent pas, car les Allemands ne devaient pas savoir qu'ils avaient décodé Enigma. Il fallait éviter que ces derniers ne recourent à d'autres formes de codage. Ainsi les chefs informés grâce à l'opération « Ultra » devaient accompagner leurs ordres d'une « cover story » crédible concernant l'origine des informations qui déterminaient ceux-ci. Cette tactique de camouflage fut si efficace que l'existence et les performances de l'Ultra restèrent absolument inconnues des Allemands. Même après la fin des hostilités, les Américains et les Britanniques gardèrent ce secret pour pouvoir éventuellement s'en resservir. Le décodage resta donc un mystère et même les experts crurent longtemps qu'Enigma était restée inviolée.

La documentation sur la guerre sous-marine à la Bibliothek für Zeitgeschichte

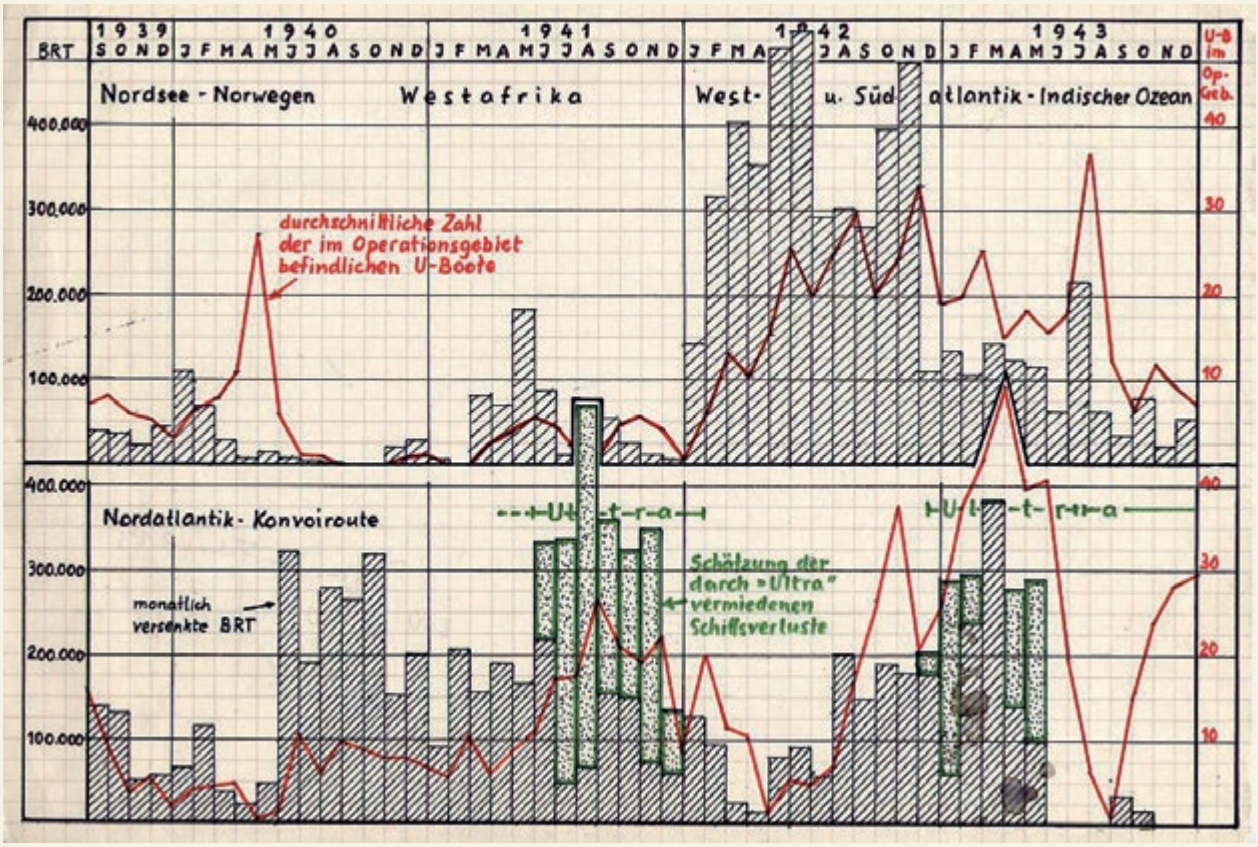
En 1959, Jürgen Rohwer fut nommé directeur de la BfZ de Stuttgart, important centre de documentation pour toutes les recherches sur la Seconde Guerre mondiale. Rohwer s'intéressait passionnément à l'histoire de la marine. Après la guerre, il soutint le travail du « Naval Historical Team », groupe d'officiers allemands qui était chargé par les Anglais et les Américains d'étudier les opérations de la marine de guerre allemande. Il rechercha partout des informations sur le domaine qui l'intéressait, celui de la guerre sous-marine allemande et de ses succès lors du torpillage de bateaux alliés. En particulier, il dactylographia en cachette le journal de guerre du chef des sous-marins, Karl Dönitz. Dönitz avait été aussi le commandant en chef de la marine de guerre et le successeur d'Hitler comme président du Reich ; Rohwer fit sa connaissance à sa sortie de prison et noua avec lui des relations d'amitié.

De 1957 à 1986, Rohwer fut le rédacteur en chef de la revue spécialisée *Marine Rundschau*. En tant que tel, il constitua dans la BfZ une importante collection autour de l'histoire de la marine, comprenant entre autres un demi-million de photos. Il prit part aussi, par de nombreuses publications, aux recherches sur la guerre en mer ainsi que sur les services secrets durant la Seconde Guerre mondiale. Grâce à un important corpus de sources premières (dénombrement des tirs de sous-marins, journal de guerre du haut commandement des sous-marins, liste dressée par l'amirauté britannique des navires perdus et autres listes nationales de pertes de bâtiments), Rohwer constitua un ensemble de plus de 18 000 cartes qui documentent une à une toutes les torpilles lâchées par les sous-marins allemands durant la Seconde Guerre mondiale. Il utilisa le matériel ainsi rassemblé dans son livre paru en 1968 et intitulé *U-Boot-Erfolge der Achsenmächte* (Victoires sous-marines des forces de l'Axe). L'analyse des données permit de constater que le torpillage des bâtiments alliés dans l'Atlantique en 1941 avait été bien inférieur à ce que le nombre des sous-marins engagés aurait pu laisser prévoir. Pour 1943, Rohwer fit les mêmes constatations (voir ill. p. 70 en haut).

Au vu de ces constats, Rohwer se demanda si le codage des messages radio de la marine allemande pendant la guerre avait été efficace. Il questionna d'importants témoins, mais ceux-ci restèrent muets et ne soufflèrent mot du projet « Ultra » toujours tenu secret. Ainsi



Graphique des batailles d'escortes dans l'Atlantique.
Mise en place d'une barrière-piège à sous-marins et dévoiement des convois alliés
(coll. Württembergische Landesbibliothek Stuttgart).



Nombre de torpillages par mois par les sous-marins allemands entre 1939 et 1943
(coll. Württembergische Landesbibliothek Stuttgart).

Symposium international sur le décodage radio durant la Seconde Guerre mondiale, Bonn et Stuttgart, 1978. Le troisième à partir de la droite est Jürgen Rohwer
(coll. Württembergische Landesbibliothek Stuttgart).

Stephen Roskill, auteur d'une histoire officielle de la guerre navale britannique, avait rendu public dans un livre de 1959 le fait que les Anglais, au moment de la capture du sous-marin allemand U-110, avaient mis la main sur d'importants documents concernant l'appareil Enigma. Mais même après plusieurs bouteilles de vin, Rohwer ne parvint pas à faire avouer à Roskill que les Anglais avaient réussi un décodage grâce à ces documents ; comme les autres historiens, il pensa donc que les repérages radio par terre et les « high frequency direction finder » des bâtiments d'escorte avaient été la cause des échecs de plus en plus nombreux des Allemands dans la guerre sous-marine.

La grande révélation

En automne 1974 eut lieu un événement qui fit sensation chez les historiens : le commandant d'aviation Frederick W. Winterbotham dévoila dans son livre *The Ultra Secret* (Le secret Ultra) le « secret le mieux gardé de la Seconde Guerre mondiale ». Par ailleurs, en 1976, les gouvernements britannique et américain mirent à la disposition des chercheurs les archives « Ultra ». S'ensuivirent d'intenses travaux auxquels participa Rohwer. En 1978, il organisa un grand congrès international à Bonn et à Stuttgart sur le thème du codage et du décodage radio pendant la Seconde Guerre mondiale (voir ill. ci-contre, en bas). D'importants témoins et historiens venus de la République fédérale d'Allemagne, d'Angleterre, des États-Unis, du Canada, de Pologne, de France, de Finlande et de Suisse s'y retrouvèrent pour discuter de l'importance d'Ultra. Les conférences et les discussions furent publiées en 1979 dans le livre *Die Funkaufklärung und ihre Rolle im Zweiten Weltkrieg* (Le décodage radio et son rôle dans la Seconde Guerre mondiale). Par la suite, Rohwer continua ses recherches concernant les problèmes radio et autres activités de renseignement. En reconnaissance du rôle qui fut le sien dans ces recherches, il fut nommé vice-président de la Commission internationale d'histoire militaire, fonction qu'il exerça de 1985 à 2000, et de 1993 à 1999, il fut président d'une association qui venait d'être créée, l'International Intelligence History Association. Rohwer mourut en 2015 à 91 ans. En 1978, au moment où se tenait le congrès à Stuttgart, la BfZ présenta une exposition sur le thème du codage et du décodage durant la Seconde Guerre mondiale. À cette occasion, on fit l'acquisition d'une machine Enigma. Elle figurait aussi dans l'exposition « Cent ans de la Bibliothek für Zeitgeschichte. 1915-2015 », qui a été présentée jusqu'au 9 avril 2016 à la Württembergische Landesbibliothek.

Christian Westerhoff, Thomas Weis
(traduction Françoise Bornemann)

ORIENTATIONS BIBLIOGRAPHIQUES :

— Bertrand, Gustave, *Enigma ou la plus grande énigme de la guerre 1939-1945*, Paris, 1973

— Erskine, Ralph, « Enigma's Security. What the Germans really knew », in Michael Smith / Ralph Erskine (éd.), *Action this day*, London, 2001, p. 370-385

— Rohwer, Jürgen, « Der Einfluss der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges », in *Vierteljahrshefte für Zeitgeschichte*, 27, 1979, H. 3, p. 325-369

— Rohwer, Jürgen, *Die U-Boot-Erfolge der Achsenmächte 1939-1945*, München, 1968

— Rohwer, Jürgen, « Vom Naval Historical Team zum Arbeitskreis für Wehrforschung », in Hartmut Klüver / Thomas Weis (éd.), *Marinegeschichte - Seekrieg - Funkaufklärung. Festschrift für Jürgen Rohwer*, Düsseldorf, 2004, p. 79-88

— Rohwer, Jürgen / Jäckel, Eberhard (éd.), *Die Funkaufklärung und ihre Rolle im Zweiten Weltkrieg*, Stuttgart, 1979

— Roskill, Stephen Wentworth, *The secret Capture*, London, 1959

— Weis, Thomas, « Jürgen Rohwer, die Bibliothek für Zeitgeschichte und das Marinearchiv im Kalten Krieg », in Christian Westerhoff (éd.), *100 Jahre Bibliothek für Zeitgeschichte. 1915-2015*, Stuttgart, 2015, p. 108-127

— Winterbotham, Frederick William, *The Ultra Secret*, London, 1974