Zdzisław J. KAPERA[1]

Le décryptage d'Enigma et son rôle dans la Seconde Guerre mondiale

ENIGMA : une machine chiffrante ultra-performante

Au début du XX^e^ siècle quelques inventeurs avaient cherché à construire une machine sûre et performante à base de tambours (ou roues) chiffrants appelés rotors. En 1919, à l'issue de la Grande Guerre, l'ingénieur hollandais Hugo Koch avait pris le premier un brevet pour une machine à écrire secrète. Mais ce fut un ingénieur allemand, Arthur Scherbius, auquel Koch avait cédé ses brevets, qui en construisit le prototype. Son entreprise fut un échec commercial, mais attira l'attention de la Reichmarine (1926) et de la Reichswehr (1928) qui l'utilisèrent pour le chiffrement mécanique des messages destinés ensuite à être transmis par radio. Entre 1937 et 1938, les unités de l'Abwehr (services d'espionnage militaire), de la SD (services de sécurité), les postes et les chemins de fer allemands furent équipées de machines *Enigma*[2]. Parmi les spécialistes, la version militaire d'*Enigma*, sans cesse modifiée, passait alors pour une machine impossible à *casser*, à l'abri de toute tentative de décryptage. Les Français et les Anglais s'attaquèrent au système, en vain. Même équipés de documents allemands originaux (description, mode d'emploi, système de la configuration des rotors pour 3 mois et – probablement – un message clair accompagné du texte codé) qui leur avaient été transmis par un membre du Chiffrierstelle (agence cryptologique de la Reichwehr), ils n'arrivèrent pas à violer le secret d'*Enigma*. Heureusement, l'officier qui avait acheté ces documents avait des relations au Bureau des Chiffres polonais de la deuxième section des services de renseignements; en automne 1932, ils furent remis à un jeune mathématicien, Marian Rejewski. Ce fut un coup dans le mille ! La formation très solide de cet ancien étudiant de l'Université de Poznań, le stage d'un an qu'il avait effectué à la chaire des statistiques de l'université de Göttingen, un cours de cryptologie qu'il avait suivi, une parfaite connaissance de l'allemand, mais avant tout une extraordinaire intuition, autant d'atouts qui lui permirent d'abord de faire une reconstruction mathématique des connexions internes des câbles d'*Enigma* à partir d'éléments dont ils disposait, et d'effectuer ensuite vers la fin de l'année un premier décodage réussi. Il n'est pas sans importance de rappeler qu'un mois après, le 30 janvier 1933, Adolf Hitler devint chancelier du troisième Reich. On peut donc

[1] Docteur ès sciences, archéologue, responsable de la Bibliothèque de l'Institut d'Orientalisme de l'Université Jagellon.
[2] Concernant la première période de l'histoire de l'*Enigma*, voir D. Kahn, *Seizing the Enigma*, Houghton Mifflin Co. : Boston 1991, chapitre 3, pp. 31-48.

dire que, même si nous n'avons pas eu *notre espion chez Hitler*[3], pour paraphraser le titre de l'excellent livre du colonel Paillole, *Enigma* s'y est en quelque sorte substituée.

Entre 1933 et 1938, Rejewski et ses deux collègues du BS-4 (section allemande du Bureau des Chiffres polonais), Jerzy Różycki et Henryk Zygalski, cassèrent de façon suivie, sans interruptions, des codes d'*Enigma*, grâce à quoi la Deuxième Section put être au courant des efforts de réarmement de la Wehrmacht, de la Luftwaffe et de la Kriegsmarine[4]. Chaque division nouvelle, terrestre ou aérienne, chaque navire de guerre nouveau étaient équipés d'une machine *Enigma*. Il y avait de quoi écouter ! En fait, des stations d'écoute radio situées à Krzesławice près de Cracovie, à Poznań et à Varsovie assuraient une interception régulière de messages allemands. En janvier 1938, un test effectué pendant deux semaines démontra que le Bureau des Chiffres sut casser 75 pour cent des messages interceptés[5]. Ce résultat excellent aurait pu être encore meilleur, selon Rejewski, si les Polonais avaient disposé d'une meilleure écoute radio (certains messages avaient été incomplets ou mal transcrits par les radiotélégraphistes) et d'équipes de cryptologues plus importantes. Malheureusement, ceux-ci ne furent pas nombreux au BS-4[6].

La gloire, à d'autres?

Les historiens s'accordent à croire qu'*Enigma* a joué un rôle considérable dans l'histoire de la seconde guerre mondiale. Cette opinion est confirmée par l'observation que le général Dwight D. Eisenhower, chef des Alliés et futur président des Etats-Unis, exprima dans une lettre du 7 juillet 1945, adressée au général Stewart Graham Menzies, chef des services secrets britanniques. (La copie de cette lettre se trouve à la bibliothèque présidentielle d'Eisenhower). Citons-en quelques extraits : *„Les informations fournies par vos services de renseignements avant, pendant et après cette campagne [il s'agit de l'opération Overlord, c'est-à-dire du Débarquement de Normandie] ont été pour moi très précieuses. Elles ont grandement simplifié ma tâche de commandant en chef des forces armées. Elles ont sauvé la*

---

[3] Voir P. Paillole, *Notre espion chez Hitler*, Éditions R. Laffont : Paris 1985.
[4] Voir J. Garliński, *Intercept. The Enigma War*, J. M. Dent, London 1979 et W. Kozaczuk, *Enigma. How the German Machine Cipher Was Broken*, and *How It Was Read by the Allies in World War Two*, University Publications of America : [Washington] 1984.
[5] J. Tebinka, Account of the Former Chief of Polish Intelligence on Cracking the *Enigma* code of 31 V 1974 [dans:] Marian Rejewski 1905-1980. Living with the *Enigma* Secret, Ed. by J. S. Ciechanowski et al., Bydgoszcz City Council, Bydgoszcz 2005, pp. 201-216 (voir p. 210). Le document de National Archives, Public Record Office (Kew), HW 25/16. Cf. également H. Hinsley, The Polish, French and British Contributions to the Breaking of the *Enigma* [= Appendix 1 in:] H. Hinsley et al., British Intelligence in the Second World War. Its Influence on Strategy and Operations, Vol. 1, HMSO, London 1979, pp. 487-495 (cf. p. 490).
[6] M. Rejewski, *How the Polish Mathematicians Broke Enigma* [dans:] W. Kozaczuk, *Enigma*, pp. 246-271 (cf. p. 265).

vie de milliers d'êtres humains et contribué à réduire le temps nécessaire pour mettre en déroute l'ennemi et le sommer de se rendre". Il prie Menzies de transmettre *„personnellement et à chacun qui a été engagé dans ce travail, l'expression de son admiration la plus profonde et ses remerciements pour sa contribution décisive à l'effort militaire des Alliés"*[7].

On ignore si le général Menzies avait transmis ces paroles à ses cryptologues, s'il leur avait fait voir l'original de la lettre. Peut-être pas, car le commandeur Frederick W. Winterbotham, un des proches collaborateurs du général et auteur du système de distribution des informations reçues grâce au décodage d'*Enigma*, cita ces propos à partir d'une copie de la lettre se trouvant aux Etats-Unis. Ce dont on peut être absolument sûr, c'est que Menzies ne l'avait jamais montrée ni aux cryptologues polonais ni à leurs chefs, sans lesquels le succès du décryptage n'aurait pas été possible. Et pourtant, ils étaient en Angleterre depuis deux ans ! Le général Menzies n'a même pas autorisé les membres de l'équipe polonaise, qui avaient gagné l'Angleterre en août 1943, à joindre l'équipe de Bletchley Park [8] !

Il n'a pas fait partager la gloire aux autres. Il en a cueilli les fruits tout seul. Le 1er février 1943, il a été décoré des médailles de saint Michel et de saint Georges et s'est vu décerner un titre de noblesse. Grâce à ses mérites de guerre, Menzies a continué d'être le chef des services secrets britanniques qu'il n'a quittés qu'en 1952, de son propre gré et au sommet de la gloire. L'affaire de Kim Philby, qui l'aurait certainement compromis, n'a éclaté que huit ans plus tard[9].

Le dévoilement progressif des secrets d'*Enigma*.

Les cryptologues polonais qui ont apporté une contribution précieuse à l'opération Ultra étaient restés dans l'oubli. Jusqu'à sa mort en 1968, le général Menzies n'en avait rien dit, de même qu'il n'avait pas dispensé ses cryptologues du serment qu'ils avaient prêté de garder secrets tous les détails de l'opération Ultra. Ses successeurs en avaient fait autant. Le secret d'*Enigma*, bien que connu d'une bonne dizaine de milliers de personnes employées à Bletchley Park et de quelques centaines d'officiers du MI6, n'a été révélé que 30 ans après la guerre. En Pologne le colonel Władysław Kozaczuk de l'Institut militaire historique a fait publier en 1967 l'ouvrage intitulé *Bataille des secrets*, consacré à l'histoire des services de

[7] Cf. F. Winterbotham, *The Ultra Secret*, Futura : London 1975, p. 18.
[8] D'après Alan Stripp *"Setting them* [M. Rejewski and H. Zygalski, after 1943] *to work on the Doppellkasseten system was like using racehorses to pull wagons"* (A. Stripp, "*A British Cryptanalyst Salutes the Polish Cryptanalysts"*, *The Enigma Bulletin* No. 3, May 1998, pp. 1-3, cf. p. 2).
[9] A. Cave Brown, *"C". The Secret Life of Sir Stewart Menzies*, Macmillan : New York 1987, passim.

renseignement polonais entre 1922 et 1939. Ce livre révèle *„le déchiffrement par des cryptologues polonais la machine chiffrante Enigma ce qui permit de lire nombre de messages considérés par l'état-major allemand comme totalement protégés contre le déchiffrement",* et *„le travail des stations d'écoute installées par les services de renseignement radio et des cellules du Bureau des Chiffres* [qui]*... constitua un apport précieux à la reconnaissance du développement des forces armées allemandes*"[10]. Le livre de Kozaczuk a trouvé un écho en Allemagne : *Die Nachthut*, journal des anciens membres de l'Abwehr en a publié de longs extraits, mais a contesté la thèse de l'auteur selon laquelle les Polonais auraient décrypté *Enigma*[11]. Ce qui est étonnant, c'est que même Kozaczuk ne connaissait pas à l'époque les noms des décrypteurs polonais.

L'année suivante parut le livre de l'historien britannique David Irving sur le Forschungsamt, la Section du Chiffre dirigée par Hermann Göring lui-même. L'auteur de l'introduction à *Breach of Security* (London 1968), Donald Cameron Watt, professeur à l'Université de Londres, y a révélé un fait jusque là complètement méconnu. Sans mentionner le nom d'*Enigma*, il a informé le public que la Grande Bretagne *„avait reçu des services de renseignement polonais les clés de chiffres militaires et diplomatiques allemands"*[12]. Ce texte, même s'il ne mentionnait ni le nom du centre de cryptologie et de repérage radio polonais de Pyry ni la date de la transmission des clés (juillet 1939), a tout de même levé le voile du secret. Pourtant, cette révélation n'a suscité aucune réaction de la part de ceux qui détenaient le secret *„du canard qui ne cancanait pas mais pondait des oeufs d'or"* (paroles de Winston Churchill)[13]. Les initiés devaient se taire et ils persistaient dans leur mutisme.

Or, le hasard a voulu qu'un jour le général français Gustave Bertrand, ayant dans sa jeunesse collaboré avec les cryptologues polonais, avant de monter dans un train a acheté à la gare le livre de Michel Garder sur les services secrets de son pays (*La guerre secrète des services spéciaux français 1935-1945*, Paris 1967). Scandalisé par la façon dont l'auteur avait décrit le travail du renseignement radio qu'il avait dirigé avant la guerre et pendant la campagne 1939-40, il a décidé de présenter sa version des faits[14], tout en protégeant la confidentialité de son agent allemand, de ses collaborateurs et collègues et sans révéler les noms des cryptologues polonais. Dans un livre publié en 1973 qui est passé inaperçu en

[10] Cf. W. Kozaczuk, *Bitwa o tajemnice [Bataille des secrets]*, Książka i Wiedza, Warszawa 1967, pp. 127-128.
[11] Cf. W. Kozaczuk, *W kręgu Enigmy [Autour d'Enigma]*, Książka i Wiedza, Warszawa 1986, 2e ed., p. 11.
[12] Cf. la nouvelle édition, malheureusement sans l'introduction, D. Irving, *Das Reich hört mit*, Arndt, Kiel 1989.
[13] O. Hoare, *Enigma. Codebreaking and the Second World War*, Public Record Office, Kew 2002, p. 11.
[14] Cf. G. Bertrand, *Enigma ou la plus grande énigme de la guerre 1939-1945*, Plon : Paris 1973, pp. 13-14 et 265-267.

France, mais a suscité un vif intérêt en Pologne, général Bertrand décrit ses contacts avec le Bureau des Chiffres polonais, révèle la transmission du secret du décryptage d'*Enigma* aux Alliés en juillet 1939. Il y parle du succès de la collaboration polono-franco-britannique durant la campagne 1940 et de ses efforts pour continuer les travaux cryptologiques en zone libre, toujours en collaboration avec les Polonais. Malheureusement, le livre de Bertrand, mal écrit, mal rédigé, plein de lacunes, a raté la chance de devenir un bestseller. Et pourtant, il en avait le potentiel ! Même son titre intriguait : *Enigma ou la plus grande énigme de la guerre 1935-1945,* (Paris 1973). Par une coïncidence singulière, le livre parut dans les librairies parisiennes juste après Noël 1972, quarante ans jour pour jour après la reconstruction mathématique des clés d'*Enigma* par Marian Rejewski, employé à la section allemande du Bureau des Chiffres polonais. D'après les paroles de celui-ci, il avait eu l'intuition de vérifier sa découverte, sachant qu'en cette période de fêtes de fin d'année 1932 les Allemands allaient s'adresser des voeux de Noël. Et, comme par un coup de baguette magique, à travers les messages codés ont surgi des textes clairs de dépêches secrètes[15] ! Il serait intéressant de savoir si la date de parution du livre de Bertrand fut choisie délibérément pour rappeler celle du décodage d'*Enigma* ou si c'était une pure coïncidence.

Frederick W. Winterbotham, commandant en chef de l'opération Ultra, ne connaissait probablement pas le livre de Bertrand[16], car sa version de la collaboration cryptologique des Alliés dans les années 1939-1940 est loin d'être exacte[17]. Lui-même, tout comme Gordon Welchman, excellent cryptologue de Bletchley Park, devenu par la suite expert de la protection des ordinateurs, employé dans les années 70. à la corporation américaine MITRE[18], se sont battus pour obtenir l'autorisation de faire paraitre leurs mémoires, dans lesquels l'affaire d'*Enigma* allait occuper une place de choix. Ils se rendaient bien compte qu'après la révélation par J. C. Masterman des opérations du XX-Committee (retournement de presque tous les agents nazi en Grande Bretagne)[19], il fallait continuer de révéler la vérité sur les activités de l'Intelligence Service britannique pendant la seconde guerre: *Enigma* devait être

[15] Cf. M. R. D. Foot, « Boże Narodzenie do rozszyfrowania [Noël est nécessaire pour déchiffrer] », *Rzeczpospolita,* 13-14 Juillet 2002.
[16] Cf. note 6.
[17] Malgré cértaines réserves, Winterbotham n'a pas changé son opinion quant à la contribution des Polonais. (Cf. les corrections de M. Z. J. Kapera dans son article *The Polish Success with Enigma in British Literature* [dans:] W. Kozaczuk, J. Straszak, *Enigma. How the Poles Broke the Nazi Code*, Hippocrene Books : New York 2004, pp. 127-153 (cf. pp. 136-139).
[18] Cf. M. Baldwin, *Gordon Welchman. A biographical note* [in:] G. Welchman, *The Hut Six Story. Breaking the Enigma Codes*, M & M Baldwin, Cleobury Mortimer : Shropshire 1998, 2e ed., pp. 250-251.
[19] J. C. Masterman, *The Double Cross System in the War of 1939-1945*, Yale University Press : New Haven 1972.

l'étape suivante de ces révélations. Les éditeurs, grandes sociétés anglo-américaines, ont soutenu les deux auteurs dans leurs efforts d'obtenir l'autorisation de publier. Mais le chef du General Communication Head Quarter, sir John Hooper, ainsi que les responsables du renseignement au niveau du gouvernement (ministère des Affaires étrangères, ministère de la Défense) leur ont catégoriquement refusé leur autorisation. Dans cette situation, celui qui a finalement révélé le secret d'Enigma et de l'opération Ultra fut Anthony Cave Brown, journaliste américain de renommée internationale (mort tout récemment). Dans son livre *La guerre secrète* (Paris, 1982, le titre original *Bodyguard of lies,* première édition Harper and Row, New York 1975) Brown a donné une description minutieuse du plan de désinformation allié lors du Débarquement de Normandie (opération Overlord). Quant à Winterbotham, le moratoire forcé sur son livre *The Ultra Secret* (London 1974, paru en France chez Robert Laffont sous le titre *Ultra*, Paris 1976) allait bientôt être levé et le livre a eu un énorme succès de librairie (plusieurs millions d'exemplaires vendus). En revanche, la publication de Welchman sur le travail des cryptologues de Bletchley Park, qui n'a vu le jour qu'en 1982, a brisé la carrière de son auteur. Le bras de la direction du GCHH a été si long que Welchman, qui travaillait aux Etats-Unis, s'est vu retirer l'accès aux secrets de communication de ce pays. En conséquence, il ne put plus exercer son métier. Il fut frappé de cette sanction malgré (ou peut-être *à cause de*) ses mérites de guerre en domaine de décryptage, qui furent honorés de la plus haute décoration anglaise, Order of the British Empire ! Pour comble de malheur, son livre, mal conçu par l'éditeur américain, grossi de rapports des travaux que Welchman avait effectués aux Etats-Unis après 1945, n'a pas apporté à son auteur le succès qu'il méritait bien plus que l'auteur d'*Ultra*.

Les machines chifffrantes *Enigma* que les Alliées avaient prises comme butin de guerre aux Allemands en 1945 ont été remises par les Anglais aux ambassades intéressées. C'était l'argument majeur dont ceux-ci se sont servis pour justifier l'ordre de maintenir secrète toute information sur *Enigma* et l'interdiction de toute publication sur la machine[20]. Les Américains s'étaient eux aussi engagés à garder le secret d'*Enigma* aussi longtemps que les Anglais en auraient besoin ; même dans l'ouvrage de Masterman sur les agents retournés, édité par la prestigieuse Yale University Press en 1972 il n'était question que de *moyens de communications spéciaux*. D'autre part, l'absence de censure préventive aux Etats-Unis empêcha l'arrêt d'impression de l'ouvrage déjà cité d'A. C. Brown, qui allait donc paraître en

[20] D. Hooper, Official Secrets. *The use and abuse of the Act*, Secker & Warburg, London 1987, p. 197. Concernant l'affaire, cf. pp. 196-199.

1975. Brown, qui dans cette publication consacra une place considérable à *Enigma*, fut par ailleurs l'un des premiers lecteurs du manuscrit dactylographié du livre de Winterbotham *The Ultra Secret*.

Les conséquences du relâchement des restrictions par le renseignement britannique

La levée du secret acquise grâce à la publication de Winterbotham a eu une grande importance. Les efforts pour obtenir l'autorisation de publier les livres de Masterman, Winterbotham et Welchman ont contribué à ouvrir aux historiens de la seconde guerre l'accès aux documents extrêmement importants, qui sans cela auraient vu le jour bien plus tard, peut-être jamais... C'est grâce à eux que l'équipe de Harry Hinsley, ancien recteur de St. John's College à Cambridge, a pu avoir accès à la presque totalité des archives du renseignement britannique de Public Records Office (Kew), à partir desquelles ces chercheurs ont élaboré une publication en plusieurs volumes relatant la contribution du service de renseignement britannique à la stratégie et au déroulement de la Seconde Guerre mondiale. Dans cet ouvrage imposant, l'histoire est présentée de manière impersonnelle, comme celle de comités et non pas de personnes. Même dans l'appendice du premier volume (1979), où il est question de la collaboration cryptologique des Britanniques avec les Polonais et les Français, les noms des mathématiciens polonais casseurs de codes d'*Enigma* n'ont pas été cités[21]. Voilà à quel point sir Harry Hinsley, ancien employé de Bletchley Park, tenait à respecter rigoureusement les consignes gouvernementales relatives à l'histoire officielle du renseignement britannique !

Qui donc a tiré de l'oubli les décrypteurs polonais, Marian Rejewski, Jerzy Różycki et Henryk Zygalski ? Le premier qui révéla ces noms fut David Kahn, excellent historien spécialisé dans la cryptologie. Dans une note critique du livre de Winterbotham, publiée dans The *New York Times Book Review* du 29 décembre 1974[22], il présenta au public américain les trois noms, injustement oubliés par Winterbotham et fit mention de la transmission aux Alliés par les Polonais de codes *Enigma* en juillet 1939, fait historique également omis par celui-ci.

En Pologne, à la même époque, Władysław Kozaczuk commença à publier dans l'hebdomadaire *Stolica* (fin 1974 – 1975) une première version de son livre *Enigma*, grâce auquel le public polonais put enfin connaître les noms des trois cryptologues[23].

---

[21] Concernant l'appendix 1, cf. note 4.
[22] Reimprimé dans D. Kahn, *Kahn on Codes. Secrets of the New Cryptology*, Macmillan : New York 1983, pp. 211-213.
[23] W. Kozaczuk, *W kręgu Enigmy [Autour de l'Enigma]*, Książka i Wiedza, Warszawa 1979.

La source Wicher (jusqu'en 1939)

En même temps, des questions douloureuses commencent à être posées : depuis qu'on sait que la machine *Enigma* avait été reproduite en Pologne, qu'on en produisait des répliques, que les Polonais décryptèrent pendant près de 10 ans des messages chiffrés de l'armée allemande, dont aussi ceux de la marine et des forces de l'air, alors pourquoi la connaissance de ce secret ne les a-t-elle en rien aidés en 1939, pourquoi ils ont transmis ce secret aux Alliés sans rien demander en retour[24] ? En quoi le décryptage d'*Enigma* a-t-il réellement influé sur les opérations militaires de la Seconde Guerre ?

En 1939, Wicher, formidable source d'informations reçues à partir du décodage d'*Enigma*, s'est quasiment tarie[25] à la suite des changements radicaux introduits par les Allemands le 15 décembre 1938. Ceux-ci ont ajouté deux rotors supplémentaires au jeu de trois utilisés jusqu'alors et augmenté le nombre de connexions placées à l'avant de la machine de 6 à 12, ce qui a considérablement réduit la possibilité de restituer la configuration initiale déterminée par la clé secrète qui changeait chaque jour. D'après les calculs de Rejewski lui-même, lui et ses collègues ne parvenaient plus à décrypter que dix pour cent des messages interceptés. Les Polonais ont eu beau restituer rapidement le système de connexions des nouveaux rotors, car le nombre de permutations des connexions a augmenté de façon dramatique. Pour les restituer il fallait plus de bombes, c'est-à-dire de machines électromécaniques permettant d'identifier la configuration du jour et de feuilles perforées (baptisées grilles de Zygalski), correspondant à toutes les permutations du réglage de base des rotors. D'après Rejewski, « *l'usine AVA a fourni un petit nombre de rotors IV et V pour les machines servant à déchiffres les messages du réseau SD, mais pour une bombe il fallait 36 rotors IV et V, et comme le travail avec les bombes devait durer 24 heures sur 24, on avait besoin d'opérateurs supplémentaires. Et pour nos deux paquets de feuilles perforées, il en fallait 58 d'autres... Nous parvenions à décrypter les messages militaires seulement lorsque dans la machine il n'y avait par hasard que trois tambours initiaux sur un axe, ce qui arrivait en moyenne une fois sur dix* »[26]. Le colonel Jan Leśniak, chef du service *Allemagne* de la deuxième Section, a confirmé dans un entretien accordé à Ryszard Woytak le 15 janvier 1976

[24] Z. J. Kapera, ed., *Wkład polskiego wywiadu w zwycięstwo aliantów w II wojnie światowej [Contribution des Services de Renseignement Polonais pour la Victoire des Alliées dans la Seconde Guerre mondiale]*, Wydawnictwo Polskiej Akademii Umiejętności : Kraków 2004.
[25] Cf. Mon article *September 1939: the Critical Month in the History of the Polish SIGINT (German Front)* publiée dans Z. J. Kapera, *Before ULTRA There Was GALE*, The *Enigma* Press : Kraków-Mogilany 2002 [= The *Enigma* Bulletin, No. 6], pp. 53-71.
[26] M. Rejewski, *How the Polish Mathematicians Broke Enigma* [dans:] W. Kozaczuk, *Enigma*, pp. 268-269.

qu'en 1939 les officiers de l'état-major polonais avaient reçu très peu d'informations d'*Enigma*. Pendant les mois qui ont précédé le début de la guerre jusqu'en septembre 1939, l'exploration de cette source de renseignements a donc été très faible. Plusieurs raisons expliquent cette perte d'efficacité. D'abord, l'insuffisance de moyens financiers pour répondre aux besoins des cryptologues. Ensuite, le fiasco de la conférence de cryptologues alliés qui s'est tenue à Paris en janvier 1939[27] ; les Français et les Anglais avaient trop peu d'informations sur le fonctionnement d'*Enigma* pour venir en aide aux Polonais ; ceux-ci ont donc résolu de ne pas révéler à leurs homologues alliés les résultats obtenus par le BS-4.

Il faut noter cependant que les cryptologues polonais avaient fourni les clés du réseau SD de façon ininterrompue jusqu'au premier juillet 1939[28]. Cela est important dans la mesure où l'erreur courante des historiens de cette période[29] est d'affirmer qu'en 1939 le décryptage d'*Enigma* fut quasiment abandonné. Or, les services de renseignements polonais avaient été coupés d'informations provenant de cette source seulement en été 1939.

Effets à long terme de la conférence des cryptologues alliés à Pyry

Six mois après la conférence de Paris, à Pyry, près de Varsovie, s'est tenue une deuxième conférence de cryptologues alliés (du 25 au 27 juillet 1939). Les invités furent accueillis par le chef du Bureau des Chiffres, colonel Gwido Karol Langer, accompagné de son adjoint, commandant Maksymilian Ciężki. Parmi les invités, il ya eu commandant Gustave Bertrand du centre de repérage radio du Service de Renseignement français et son excellent cryptologue, capitaine Henri Braquenié. Les Britanniques furent représentés par Alastair Denniston, chef du service de déchiffrement de l'Intelligence Service (Governement Code and Cypher School), Alfred Dillwyn Knox, éminent spécialiste d'*Enigma*, et Edward Travis, chef du service repérage radio de l'Amirauté. Les Polonais ont transmis à leurs futurs compagnons d'armes les résultats de dix ans de recherches sur *Enigma* et promis de leur remettre par le courrier diplomatique deux exemplaires de la copie polonaise de la machine (un pour les Français, un autre pour les Britanniques). En plus, les Anglais allaient recevoir un paquet de grilles de Zygalski. Lors de la conférence, Marian Rejewski a eu l'honneur de

---

[27] Cf. G. Bertrand, *Enigma*, pp. 57-58, ma brochure (en préparation pour 2007) concernant les réunions des cryptographes alliées à Paris et à Pyry (Varsovie), et mon article *Paryż 1939 : Tajna konferencja kryptologów alianckich [Paris 1939. Le Conférence Secret des Cryptologues Alliées]* présentée à Słupsk (Stolpen) dans 2005. Cf. aussi H. Foss, *Reminiscences on Enigma* [dans:] R. Erskine and M. Smith, eds., *Action This Day*, Bantam Press : London 2001, pp. 45-46 ; G. Bloch, "The French Contribution to the Breaking of '*Enigma*'", *The Enigma Bulletin* No. 1, Dec. 1990 [The *Enigma* Press, Cracovie], p. 12-13.

[28] Cf. M. Rejewski, *How ...*, p. 269.

[29] Rejewski d'après P. Calvocoresi, *Top Secret Ultra*, Cassel, London 1980.

présenter à A. D. Knox les résultats de ses découvertes sur *Enigma*[30]. Le célèbre cryptologue britannique n'arrivait pas à croire qu'il avait été si près de trouver la clé de l'énigme. Or, « *les miracles n'arrivent qu'une fois* », comme a très justement remarqué à ce propos Gilbert Bloch, spécialiste le plus connu aujourd'hui de l'histoire d'*Enigma*[31]. En effet, à partir des données qui depuis 1932 furent en possession de tous les cryptologues, seul Rejewski a su déchiffrer les codes secrets.

La transmission du secret aux Alliés a été la seule décision raisonnable à prendre à la veille de la guerre. D'après le colonel Stefan Mayer, elle aurait été prise au niveau du chef de l'Etat-major polonais. Je doute fort que le général Wacław Stachiewicz en ait compris l'importance ou qu'il ait été capable d'en prévoir les effets à long terme. Pour lui, ce fut une décision plus politique (un geste de solidarité à l'égard des Alliés) que militaire. Dans son rapport sur les préparatifs à la guerre concernant la période 1935-1939, on chercherait en vain une seule mention de la II^{e} Section ou du Bureau des Chiffres[32]. Il est mort en 1973, parfaitement inconscient de la plus grande réussite de ses subalternes[33].

Les cryptologues polonais pendant la guerre

Le secret d'*Enigma* fut donc généreusement transmis aux Alliés, sans rien leur demander en retour. La suite de cette histoire est connue du public polonais grâce aux ouvrages de Jerzy Garliński et Władysław Kozaczuk[34]. Après l'invasion de la Pologne par les troupes allemandes, les cryptologues polonais ont gagné la France et, ayant reçu le consentement du général Władysław Sikorski, se sont mis au service des Français. Ceux-ci ont entrepris la production de machines supplémentaires, indispensables pour les travaux de décryptage, car les répliques polonaises avaient été complètement détruites en septembre 1939; le colonel Langer n'avait transporté à Paris qu'un exemplaire de la machine. Les Anglais ont concentré leurs efforts à mettre au point la version modifiée, plus performante, des grilles de Zygalski (baptisées Jeffrey's sheets), dont un paquet a été transmis au centre français du repérage radio au P.C. Bruno (Gretz-Armainvilliers, dans la région parisienne). Grâce à cela, assez rapidement, le 17 janvier 1940, les Alliés sont parvenus à casser pour une

---

[30] Concernant le conference à Pyry, cf. J. S. Ciechanowski and E. Maresch, Disclosure of the *Enigma* Secrets to the Allies (Pyry, July 1939). Documents in the British Archives [dans:] Marian Rejewski 1905-1980. Living with the *Enigma* Secret, pp. 217-242. Ma brochure à ce sujet sera publiée en 2007.
[31] Cf. G. Bloch, *The French Contribution*, p. 12.
[32] W. Stachiewicz, *Wierności dochować żołnierskiej [Etre fidèle à son serment de soldat]*, Oficyna Wyd. Rytm, Warszawa 1998. Dans son livre de 800 pages il n'y a que quelques notes concernant le 2^{e} Bureau !
[33] Cf. les Mémoires de son fils B. Stachiewicz récemment publiée.
[34] Les livres sont mentionnés dans la note 3.

première fois le code militaire d'*Enigma*. Il s'est avéré alors qu'après le 1er septembre 1939 les Allemands n'avaient apporté aucune modification au système : *Enigma* était à la disposition des Alliés. Cependant, comme nous le savons, cet accès aux renseignements secrets des nazis n'a pas aidé les Alliés à bien déchiffrer les intentions d'Hitler à l'encontre du Dannemark, de la Norvège et plus tard de la France. Celle-ci n'a pu être sauvée, bien que, pour citer les paroles du colonel Louis Rivet, chef du P.C. Bruno, à partir du 10 mai 1940 « nous lis[ions] tout » et que se fût bien *Enigma* qui avait prévenu l'Etat-major français du décryptage du code secret français par les Allemands[35]. L'apport des services de déchiffrement d'*Enigma* pendant la Bataille de Dunkerque et la bataille d'Angleterre n'a jamais été expliqué à fond. Mais les Alliés ont rapidement appris à utiliser opérationnellement les informations fournies, grâce notamment aux efforts de Winterbotham qui a mis sur pied un système sûr et efficace de transmission des renseignements obtenus, baptisé SLU (Special Liaison Unit) et a mené à bien l'opération Ultra, c'est-à-dire la distribution des informations interceptées d'abord à partir d'*Enigma*, et plus tard aussi de Geheimschreiber[36].

Le rôle d'*Enigma*

Harry Hinsley refusa la thèse de Winterbotham, reprise par les journalistes et même par certains historiens, selon laquelle il faudrait réécrire l'histoire de la seconde guerre mondiale, car les Alliés avaient gagné celle-ci grâce à *Enigma*[37]. Bien évidemment, il n'en fut pas ainsi. Le renseignement à lui seul n'a pu gagner la guerre. Une telle thèse serait absurde. Selon Hinsley, ce qui avait déterminé le sort de la guerre, ce fut le ralliement au camp des Alliés de la Russie, agressée en juin 1941, et ensuite celui des Etats-Unis, qui avaient déclaré la guerre aux Nazis après la défaite de Pearl Harbour. Il serait difficile de ne pas se rallier à cette opinion : en effet, l'entrée en scène de ces deux pays fit pencher la balance du côté des Alliés. D'un autre côté, la guerre continua pendant quatre ans encore et son résultat resta indécis jusqu'à la fin. Et là, l'acquisition par le renseignement radio, à partir de la fin de 1941,

---

[35] Cf. P. Paillole, *Notre espion chez Hitler*, R. Laffont, Paris 1985, pp. 180-185, esp. pp. 183-184. Les citations sont tirées des carnets de colonel Rivet.

[36] Cf. F. Winterbotham, *Ultra*, R. Laffont : Paris 1976, passim.

[37] Concernant le rôle d'*Enigma*, cf. D. Kahn, Le Rôle du décryptage et du renseignement dans la stratégie et la tactique des Alliés, *Revue d'Histoire de la Deuxième Guerre Mondiale*, 28 (Juillet 1978), 73-85 ; H. C. Deutsch, « The Influence of Ultra on World War II », *Parameters*, 8 (Décembre 1978), 2-15 ; R. Bennet, *« World War II Intelligence : The Last 10 Years' Work Reviewed* », *Defence Analysis*, 3, No. 2 (Juin 1987), 103-117 ; F. H. Hinsley, *The Influence of Ultra in the Second World War* [dans :] F. H. Hinsley, A. Stripp, éd., *Codebreakers. The Inside Story of Bletchley Park*, Oxford University Press : Oxford 1993, 1-13 ; l'introduction dans D. J. Sexton, Jr., *Signals Intelligence in World War II. A Research Guide*, Greenwood Press : Westport, Conn. – London 1996, XXXIII – XL; F. H. Hinsley, *The Counterfactual History of No Ultra* [dans:] B. J. Winkel et al., *The German Enigma Cipher Machine. Beginnings, Success, and Ultimate Failure*, Artech House : Boston-London 2005, pp. 211-227.

des informations précieuses d'*Enigma* eut des conséquences remarquables. *« L'effort militaire des Alliés occidentaux sur tous les fronts... était dirigé par un accès massif, continu et souvent ininterrompu aux informations courantes concernant les dispositions, les intentions, les effectifs et les difficultés de l'ennemi. Ces informations étaient si riches, bien que jamais complètes, que, malgré des interprétations parfois fautives, les conclusions qu'on en tirait, qu'elles fussent positives ou négatives, furent le plus souvent justes. Cela permit* [aux Alliés] *non seulement de mener à bien des attaques stratégiques et d'éviter des surprises stratégiques, mais aussi de raccourcir la guerre »*, écrit Hinsley. Raccourcir ? Comment et de combien de temps ? D'un mois, d'un an, peut-être de deux ou de plus de deux ans ? Voilà la question.

Le principal changement qui fut introduit depuis l'été 1941 a été d'effectuer les opérations *militaires « de manière à réduire les coûts personnels et matériels tout en rendant la vie bien plus dure à l'ennemi »*. Et comment a-t-on réussi à raccourcir la guerre ? Là, selon Hinsley, nous sommes voués à des calculs incertains et hypothétiques, qui sont pourtant d'une importance capitale dans les présentes réflexions. D'après Hinsley, au printemps 1941, les Alliés ont réussi, grâce entre autres à *Enigma*, à traquer du cuirassé Bismarck et affaiblir la flotte italienne en Méditerranée dans la bataille victorieuse du Cap Matapan ; les informations reçues d'*Enigma* ont facilité le retrait du corps expéditionnaire sans pertes importantes, sans pour autant empêcher l'invasion de la Grèce. L'occupation de la Crète par les Allemands fut en fait une victoire à la Pyrrhus. Les Alliés ont su arrêter le général Rommel presque aux portes du Caire, grâce à la destruction de 40 à 60% de ses convois de ravitaillement, et par conséquent il ont récupéré l'Afrique du Nord et rouvert la navigation en Méditerranée déjà vers le milieu de 1943. Toujours selon Hinsley, ce fait aurait raccourci la guerre d'un an. Le déchiffrement d'*Enigma* à quatre rotors et des codes des U-boots a arrêté la domination de ceux-ci sur l'Atlantique en hiver 1941-1942, et la mise en déroute des escadres allemandes en hiver 1942-1943 a permis aux Alliés de gagner deux années supplémentaires. La suprématie militaire des Alliés lors de l'opération du débarquement de Normandie fut si fragile qu'elle *« aurait été pratiquement impossible sans les informations détaillées fournies par les services de renseignement »*. Ce qui a décidé de son succès, selon Hinsley, c'est la confiance dans la source et la connaissance exacte des forces et des plans de l'ennemi. *« Si les plans du débarquement avaient été abandonnés, celui-ci aurait pu être retardé jusqu'en 1946 ou 1947 par la mise en action de l'arme V contre le Royaume-Uni et par l'achèvement de la construction du mur de l'Atlantique, sans parler de nouveaux U-boots super-performants,*

avions supersoniques et fusées, dont l'armée allemande allait être dotée dans les premiers mois de 1945, comme l'a révélé le renseignement. Le retour sur le continent aurait donc pu être retardé jusqu'en 1948, et la victoire finale sur les Allemands n'aurait pu survenir qu'en 1949, selon des estimations très prudentes ».[38]

L'importance de l'apport polonais

La découverte du secret d'*Enigma* est un facteur qui a contribué de manière décisive au déroulement de la Seconde Guerre mondiale. Il est hors de doute que le système britannique Ultra mis en oeuvre à partir des données fournies par *Enigma* a accéléré la fin de la guerre, peut-être même de quelques années. Quelle part de cette gloire revient aux Polonais ? Hinsley reconnaît, avec réticence, que leur apport a accéléré de neuf mois[39] les travaux des Britanniques sur *Enigma*. Le neuvième mois de la guerre, ceux-ci ont pris sur un navire allemand les premiers rotors et livres de codes, ce qui de toute évidence leur aurait permis de déchiffrer *Enigma* sans recourir aux Polonais, et à cette époque là, grâce à ce butin, ils ont pu pendant quelque temps casser les messages de la Kriegsmarine. Les Britanniques semblent pourtant oublier qu'ils n'auraient pas été capables de casser eux-mêmes *Enigma*, s'ils n'avaient pas disposé des moyens (rotors et algorithmes) de configuration de la machine qu'ils avaient reçus des Polonais, même si le système polonais du décodage reposait sur le double chiffrement par les Allemands du début du message, chiffrement que ceux-ci avaient abandonné à partir du 10 mai 1940. Les Britanniques, même disposant à Bletchley Park des matériaux polonais qui leur avaient été transmis à Pyry ne sont pas arrivés à décrypter un seul message avant la mi-janvier 1940. C'est seulement l'arrivée à Paris de Turing, muni des feuilles perforées, qui a permis, grâce aux analystes polonais et à leurs collègues, de prendre contact avec le contenu des messages allemands. Or, sans une lecture ininterrompue des messages pendant quatre mois, sans connaître leur construction, leur spécificité sémantique ou les habitudes de tel ou autre chiffreur allemand, il n'aurait pas été possible de construire la bombe britannique, en mettant en profit les points faibles du renseignement radio allemand[40].

L'apport des analystes polonais dans la victoire des Alliés fut donc énorme, quoiqu'il soit toujours peu connu et apprécié.

---

[38] Les citations sont de F. H. Hinsley, *British Intelligence in the Second World War: An Overview* [dans:] B. J. Winkel et al., *The German Enigma*, pp. 117-126 [Réimpression de la "Cryptologia" 14, No. 1(Janvier 1990), 1-10.

[39] F. H. Hinsley, *British Intelligence*..., vol. 1, pp. 494-495.

[40] F. H. Hinsley, op. cit., vol. 3, 2^{e} partie, London 1988, p. 956.

Admettons que Hinsley a raison dans ses réflexions et que les efforts des cryptologues polonais ont amené à réduire la durée de la guerre de neuf mois. C'est sauver la vie de plus de trois millions de Soviétiques, car l'Union Soviétique perdait plus de cinq millions de ses citoyens chaque année de la guerre. Pour la Pologne, le nombre d'êtres humains sauvés est aussi considérable : neuf cent mille hommes ![41] Il serait intéressant de voir les mêmes estimations faites par les Britanniques, les Français, et même les Allemands. Voilà pourquoi les noms des cryptologues Marian Rejewski, Jerzy Różycki et Henryk Zygalski devraient trouver la place qu'ils méritent dans les manuels d'histoire polonaise et européenne.

Bibliographie:

Gustave BERTRAND, *Enigma* ou la plus grande énigme de la guerre 1939-1945, Paris 1973, Editions Plon.

Une mise au point indispensable. « *Enigma* » contre « The Ultra Secret » [dans :] «Bulletin de l'Amicale des Ancient Membres des Services Spéciaux de la Défense Nationale et Réseaux F.F.C. Correspondants» No. 90, II (1976), pp. 12-19.

Gilbert BLOCH, La contribution française a la reconstruction et au décryptement de l'*Enigma* militaire allemande en 1931-1932, « Revue Historique des Armées » No. 4 (Décembre 1985), pp. 17-25.

ENIGMA avant ULTRA 1930-1940, [Paris, Décembre 1985] et [Paris, Septembre 1988. Texte définitif, publication de l'auteur].

Enigma Before Ultra: Polish Work and the French Connection, „Cryptologia" 11 (1987), pp. 131-151.

Enigma Before Ultra: The Polish Success and Check, "Cryptologia" 11 (1987), pp. 227-234.

Enigma Before Ultra, "Cryptologia" 12 (1988), pp. 178-184.

The French Contribution to the Breaking "*Enigma*", "The *Enigma* Bulletin" No. 1 (Décembre 1990) [Cracovie, The *Enigma* Press], pp. 3-13.

Polish Reconstitution of the German Military *Enigma* and the First Decryptments of its Messages, "The Journal of Intelligence History" 1, No. 1 (Summer 2001), pp. 36-43.

Gilbert BLOCH et Raph ERSKINE, *Enigma*: The Dropping of Double Encipherment, "Cryptologia" 10 (1986), pp. 131-146.

[Henri BRAQUENIÉ], Interview avec le capitaine Henri Braquenié recueilli le 9 juillet 1975 a Paris [dans :] W. Kozaczuk, Geheimoperation WICHER, pp. 318-328.

Jan Stanisław CIECHANOWSKI, éd. Marian Rejewski 1905-1980, Living with the *Enigma* Secret, Bydgoszcz 2005, City Council.

Ralph ERSKINE, Z. J. KAPERA et F. WEIERUD, Pyry 1939, Kraków-Mogilany [2007], The *Enigma* Press [en préparation].

David KAHN, Seizing the *Enigma*. The Race to Break U-Boat Codes, 1939-1943, Boston 1991, Houghton Mifflin Co.

Zdzisław J. KAPERA, Before *ENIGMA* There Was GALE, Kraków-Mogilany 2002, The *Enigma* Press.

Stan badań nad polską Enigmą [w:] Z. J. Kapera, éd., Wkład polskiego wywiadu w zwycięstwo aliantów w II wojnie światowej, Kraków 2004, Wydawnictwo PAU, s. 13-26 et s. 393-400, pl. I-IV.

Marian Rejewski Pogromca Enigmy, Kraków-Mogilany 2005 et 2e édition : 2006, The *Enigma* Press.

Polish Codebreakers [dans:] Chr. H. Sterling, éd., Encyclopedia of Military Communications History, ABC-CLIO, Santa Barbara, CA. 2007 [en préparation].

[41] Cf. Z. J. Kapera, *Marian Rejewski Pogromca Enigmy [Marian Rejewski Vainqueur de l'Enigma]*, Kraków-Mogilany 2006, 2e éd., pp. 38-41(édition française en préparation pour 2007).

Władysław KOZACZUK, Geheimoperation WICHER. Polnische Mathematiker knacken den deutschen Funkschlüssel „*Enigma*“, Koblenz 1989, Bernard & Graefe Verlag.

Jean MEDRALA, Les réseaux de renseignements franco-polonais 1940-1944, Paris 2005, L'Harmattan.

L'*Enigma* polonaise en résistance a Uzès au château des Fouzes 1940 – 1942, [Uzès 2005], Société Historique de l'Uzège.

Paul PAILLOLE, Notre espion chez Hitler, Paris 1985, R. Laffont.

L'Homme des services secrets. Entretiens avec Alain-Gilles Minella, Paris 1995, Éditions Julliard.

P. RENAULD, La machine à chiffrer *Enigma*, «Bulletin Triméstriel de l'Association des Amis de l'École Supérieure de Guerre» No. 78, 1978, pp. 41-60.

L. RIBADEAU-DUMAS, Les décryptements de la machine *Enigma* des armées allemandes, Paris, Juillet 1987 [publication de l'auteur].

Jean STENGERS, *Enigma*, the French, the Poles and the British 1931-1940 [dans:] Christopher Andrew et David Dilks, The Missing Dimention, London 1984, Macmillan, pp. 126-137.

Tessa STIRLING, éd., Intelligence Co-operation Between Poland and Great Britain During World War II, vol. 1: The Report of the Anglo-Polish Historical Committee, London – Portland, Or. 2005, Vallentin Mitchell [avec contributions de J. S. Ciechanowski, E. Maresch et J. Tebinka].