



Ces Polonais qui ont décrypté Enigma

GUERRE MONDIALE • Les Renseignements polonais ont apporté un soutien essentiel aux Alliés pendant le conflit mondial. Leurs réseaux étaient non seulement très efficaces, ils étaient aussi dotés de champions du déchiffrement.

PASCAL FLEURY

HISTOIRE VIVANTE

La statue de bronze de Marian Rejewski, à Bydgoszcz (Bromberg), au nord de la Pologne, est encore régulièrement fleurie en souvenir de cet enfant du pays, héros de la Seconde Guerre mondiale. Ses faits d'armes remarquables, ce brillant mathématicien ne les a toutefois pas accomplis le fusil à la main, mais en perçant le système de codage des fameuses machines d'encryptage Enigma, largement utilisées par l'Allemagne nazie. Une découverte fondamentale, qui a permis ensuite aux services de renseignement polonais, français et britanniques de déchiffrer des milliers de messages secrets, et de donner ainsi un net avantage aux Alliés dans le conflit.

Réputée inviolable, la machine Enigma, commercialisée dans les années 1920, est employée dès 1926 par la marine allemande, puis par le reste de l'armée et les services diplomatiques, dans des versions modifiées toujours plus sophistiquées et sécurisées. L'appareil électromécanique portable, doté d'un clavier et de rotors d'encodage, sert bientôt à chiffrer et à déchiffrer pratiquement toutes les messages radio allemands ainsi que les communications télégraphiques.

Chercheurs polonais

Interceptant des messages codés devenus soudain impossibles à «casser», la Pologne voisine, qui vient d'être reconstituée en Etat après le Traité de Versailles et sert de «cordon sanitaire» pour les pays occidentaux face à l'URSS, s'inquiète de cette avancée technologique. Réalisant que pareil défi dépasse les compétences des officiers du Bureau du chiffre, le commandant Gwido Langer fait appel dès 1932 à trois jeunes mathématiciens de talent de l'Université de Pozdam: Henryk Zygalski, Jerzy Roczycycki et, le plus doué, Marian Rejewski, qui a alors 27 ans. Ce dernier se voit confier un exemplaire d'une Enigma commerciale, de nombreux textes codés allemands et des fascicules pour opérateurs transmis de France par le capitaine Gustave Bertrand, responsable de la section française de recherche de renseignements relatifs aux codes étrangers.

Comme le raconte Jean Medrala, auteur d'un des ouvrages les mieux documentés sur les réseaux de renseignements franco-



Le mathématicien polonais Marian Rejewski, honoré à Bydgoszcz (Bromberg), a été le premier à «casser» l'encryptage de l'Enigma. DR

polonais pendant la guerre¹, Marian Rejewski réussit, en seulement dix semaines, à établir la théorie mathématique du chiffrage de l'Enigma, à reconstituer les câblages internes des pièces mobiles de l'appareil et à élaborer les premières méthodes de décodage. Un prototype est réalisé par une société d'électromécanique de Varsovie, qui permet de vérifier les hypothèses émises par le jeune savant.

La «Bomba»

Entre 1934 et 1938, 17 répliques des Enigma militaires allemandes sont alors fabriquées dans le plus grand secret par l'entreprise polonaise. Les mathématiciens développent des méthodes de déchiffrement d'abord manuelles, à l'aide de cartes perforées, puis dès 1938, également mécaniques, grâce à un appareil appelé «Bomba», en raison de son cliquetis infernal. Mais les Allemands leur donnent du fil à retordre: ils modifient une nouvelle fois leurs machines en y ajoutant deux rotors d'encryptage supplémentaires, passant de

trois à cinq, forçant ainsi les chercheurs polonais à mettre au point dans l'urgence une nouvelle réplique plus complexe de la machine Enigma. C'est que le temps presse: les bruits de bottes se précisent à la frontière.

En deux ans, l'équipe polonaise a décrypté 13 000 messages

Pour ne pas risquer de perdre tous ses acquis, le Bureau du chiffre polonais décide de transmettre ses connaissances cryptographiques aux services de renseignement français et anglais. La rencontre a lieu le 24 juillet 1939 à Varsovie. Les représentants britanniques et français, totalement stupéfaits de l'état d'avancement des travaux polonais, reçoivent le descriptif détaillé de toutes les méthodes élaborées en près de dix ans, et même un exemplaire de la réplique de l'Enigma à cinq rotors.

Lorsque la Pologne est envahie par l'Allemagne et la Russie,

en septembre 1939, les officiers du Bureau du chiffre rejoignent la France, où ils sont d'abord intégrés dans l'Armée polonaise en cours de reconstitution dans l'Hexagone, puis détachés au «PC Bruno», implanté au château de Vignolles près de Paris et spécialisé dans l'écoute et le déchiffrement des messages radio de l'armée allemande.

Dès lors, les services spéciaux britanniques (cantonés à Bletchley Park près de Londres), français et polonais collaborent étroitement, se répartissant les tâches dans les activités de déchiffrement. Il s'agissait en particulier de découvrir les «clés» changées quotidiennement par les Allemands, qui conditionnaient le calibrage initial des Enigma.

Les cryptologues voient parfois leur travail facilité par des prises de guerre. Des machines Enigma ont ainsi pu être récupérées sur plusieurs sous-marins allemands capturés, comme le U-33 ou le U-110. Parfois, des

clés leur sont livrées par des agents infiltrés. Ou alors c'est la naïveté des opérateurs d'Enigma qui leur vient en aide. Par exemple lorsqu'ils terminent leurs messages par un «Heil Hitler!» ou un «Joyeux Noël!», révélant sans le vouloir une partie du codage.

Subtil double jeu

En juin 1940, lorsque la France est envahie, les cryptologues polonais et leurs collègues français du PC Bruno sont évacués vers la France libre. Une partie d'entre eux – dont les trois mathématiciens polonais – s'installent au château des Fouzes près d'Uzès dans le Gard. L'organisation, au nom de code «Cadix», est placée sous le commandement de Gustave Bertrand. D'autres spécialistes sont envoyés à Alger où ils soutiendront le major polonais Mieczyslaw Slowikowski, alias «Rygor», dans la préparation du débarquement allié en Afrique du Nord².

Au «PC Cadix», les activités de déchiffrement se poursuivent. Mais dans un double jeu des plus subtils. Car les Polonais n'ont pas

de tout envie de collaborer avec les Services spéciaux de Vichy, auxquels ils sont pourtant subordonnés. Ils leur fournissent alors des informations de moindre intérêt, tandis qu'ils renseignent abondamment le Gouvernement de la Pologne libre à Londres et ses alliés britanniques de Bletchley Park.

Grâce à sept machines Enigma reconstituées, un important volume de dépêches allemandes peut être déchiffré. Les messages proviennent de la Gestapo, de cellules clandestines allemandes agissant en France ou en Suisse, d'informateurs russes ou encore des réseaux de l'Abwehr qui suivent les bateaux alliés en Méditerranée et dans l'Atlantique Sud. En deux ans, selon le spécialiste Jean Medrala, l'équipe polonaise participe au déchiffrement de près de 13 000 messages, tandis qu'elle n'en livre que la moitié aux Services spéciaux de Vichy.

Les informations stratégiques ne sont pas toujours exploitées: il ne faut surtout pas que les Allemands se doutent des capacités de déchiffrement alliées. Ainsi, avant de bombarder un navire localisé par une dépêche, les Alliés doivent envoyer un avion de reconnaissance, censé passer «par hasard» sur les lieux. C'est lui qui avertit alors la base. Parfois, des convois sont envoyés au casse-pipe, malgré la connaissance d'un danger.

Reconnaissance tardive

Peu avant l'occupation de la zone sud, le PC-Cadix est détecté par les services allemands. Il doit être démantelé dans l'urgence. L'évacuation vers Londres, via l'Espagne, se passe plutôt mal. Plusieurs officiers sont dénoncés par des passeurs et arrêtés. Les mathématiciens Rejewski et Zygalski, internés dans un camp, n'arrivent en Angleterre qu'en été 1943. Leur compatriote Jerzy Roczycycki a moins de chance. Il meurt lors d'un naufrage après un séjour en Algérie.

A Londres, les deux cryptologues sont reçus sans honneur. Écartés du centre britannique de Bletchley Park, ils sont relégués à des travaux plus routiniers. Leurs exploits sont restés cachés pendant la Guerre froide. Ce n'est que tardivement que leur rôle déterminant dans la victoire des Alliés a enfin été reconnu. I

¹ «Les réseaux de renseignements franco-polonais, 1940 – 1944», Jean Medrala, Editions L'Harmattan, 2005.

² Voir le documentaire «Les ombres de Casablanca», le 4 décembre sur TSR2.

SEMAINE PROCHAINE

LES ENFANTS DU GOULAG

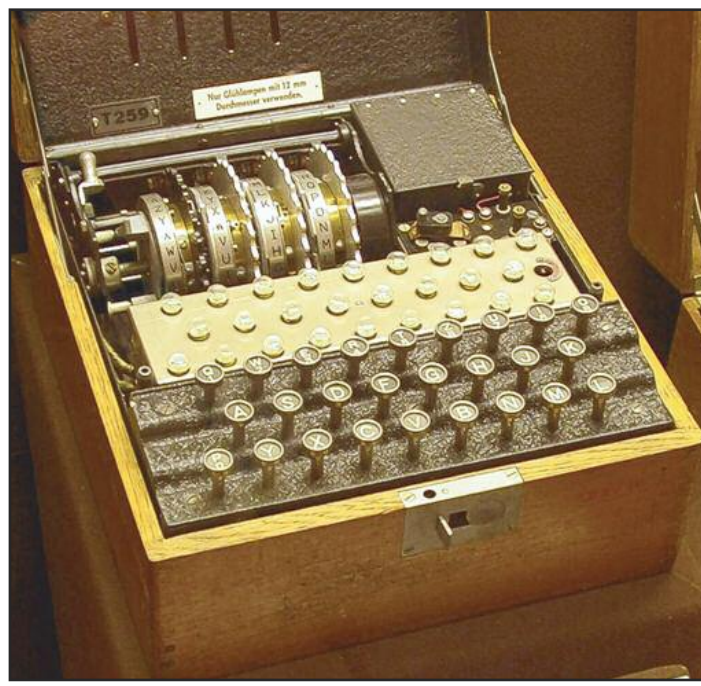
Déportés avec leurs parents ou nés au goulag parfois dans de terribles circonstances, des centaines de milliers d'enfants ont vécu dans les camps staliniens.

Vaste réseau d'espions

Ce n'est qu'en 2005, plus de 60 ans après les faits, que des historiens ont révélé un secret jusqu'ici connu des seules autorités militaires britanniques: la moitié des rapports d'espionnage reçus à Londres pendant la guerre provenait des services de renseignements polonais.

Les agents polonais opéraient sur tous les fronts, de la Scandinavie à l'Afrique du Nord. Ainsi, leur «Agence Afrika», forte de 2500 agents et informateurs, sous la direction du commandant Mieczyslaw Slowikowski, alias «Rygor», a préparé avec succès le débarquement des Alliés en Afrique du Nord, le 8 novembre 1942.

Une cellule polonaise de renseignements se trouvait aussi en Suisse. Créée par l'officier Stanislas Appenzeller, alias Etienne, elle avait des embranchements en France, Italie et Belgique. Le Réseau suisse, qui pouvait compter sur l'aide discrète du Service de renseignements helvétique, était en contact avec l'amiral allemand Wilhelm Canaris, opposé aux menées nazies. Il a ainsi pu transmettre des informations de première importance aux Alliés, comme l'attaque allemande de mai 1940 contre la France, le débarquement de 1941 de Rommel en Libye ou encore les activités des mouvements d'opposition au régime d'Hitler. PFY



ENCRYPTAGE Enigma story

Après la Première Guerre mondiale, des industriels ont eu l'idée d'utiliser une machine électromécanique pour coder leurs messages commerciaux et bancaires. La machine Enigma (DR) a été développée dès 1919 puis commercialisée par l'Allemand Arthur Scherbius. Son succès a cependant été davantage militaire que civil. La marine allemande s'y est intéressée dès 1926. Dotée de brouilleurs à 3 puis à 5 rotors, d'un clavier de 26 lettres et d'autant de voyants lumineux, elle a été exploitée jusqu'à la fin de la guerre par les pays de l'Axe, mais aussi par d'autres États, dont la Suisse. PFY