View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by OpenEdition

La revue pour l'histoire du CNRS

6 | 2002
Les années 60 : l'Espace, l'Océan, la Parole

Battle of wits: the complete story of codebreaking in World War II

Stephen Budiansky. The Free Press, New York, 2000

Jérôme Segal

Édition électronique
URL : http://journals.openedition.org/histoire-cnrs/400
ISSN : 1955-2408

Éditeur
CNRS Éditions

Édition imprimée
Date de publication : 5 mai 2002
ISBN : 978-2-271-05926-0
ISSN : 1298-9800

Référence électronique
Jérôme Segal, « Battle of wits: the complete story of codebreaking in World War II », *La revue pour l'histoire du CNRS* [En ligne], 6 | 2002, mis en ligne le 06 mars 2006, consulté le 03 mai 2019. URL : http://journals.openedition.org/histoire-cnrs/400

Ce document a été généré automatiquement le 3 mai 2019.

Comité pour l'histoire du CNRS

Battle of wits: the complete story of codebreaking in World War II

Stephen Budiansky. The Free Press, New York, 2000

Jérôme Segal

1 La construction des radars puis celle de la bombe atomique constituent deux témoignages aujourd'hui bien documentés du rôle joué par les scientifiques lors de la Seconde Guerre mondiale. Le livre de Stephen Budiansky présente la cryptologie, qui réunit la cryptographie et la cryptoanalyse, comme un autre domaine permettant d'offrir aux scientifiques mais aussi à tous les employés des centres de cryptoanalyse la place qui leur revient dans l'histoire de la guerre.

2 La bataille de l'Atlantique est la seule à avoir duré de septembre 1939 à mai 1945. Les attaques des sous-marins allemands ont considérablement affaibli les Alliés. Le déchiffrement des messages radio transmis par les Allemands a été essentiel et chaque progrès de la cryptographie allemande a eu l'effet d'un coup de pied dans les fourmilières que représentaient les centres de cryptoanalyse en Angleterre et aux États-Unis. On ne peut plus concevoir une histoire de la bataille de l'Atlantique qui ne prenne en compte ces enjeux. Des bribes de cette histoire avaient déjà été racontées, comme celle du déchiffrement à Bletchley Park, entre Oxford et Cambridge, des messages allemands. S. Budiansky revient sur le rôle primordial des mathématiciens polonais qui, comme Marjan Rejewski au début des années 1930, avaient réussi à percer le secret de l'*Enigma*, cette machine à rotor utilisée par les Allemands. David Kahn a sans doute été le premier historien de la cryptologie, à partir de la fin des années 1960, mais S. Budiansky a le mérite d'avoir dépouillé les millions de pages qui ont été rendues publiques dans les années 1990.

3 Son livre sur la « bataille des esprits » peut se lire agréablement comme un roman policier rempli d'anecdotes délectables ou encore comme une série de problèmes de logique puisque le détail technique des opérations de déchiffrement est indiqué. Les parties techniques peuvent aussi être négligées et deux idées fortes émergent alors du

livre : les conséquences de l'automatisation de la cryptoanalyse et son apport dans la prise de décision.

4 Au sujet de l'automatisation, M. Rejewski avait été le premier à construire un automate assurant le décryptage d'un message à partir d'un assemblage de plusieurs machines. Lorsque les Anglais, puis les Américains poursuivirent sur cette voie, la complexité du cryptage avait considérablement augmenté, notamment avec l'ajout de rotors sur l'*Enigma*. Une machine baptisée *Robinson* puis *Colossus*, fut construite avec une horloge interne et des tubes à vide pour un fonctionnement binaire permettant dès 1943 de déchiffrer les messages transmis par télé-imprimeur. Il s'agit d'un ancêtre des ordinateurs actuels, souvent oublié en raison du peu d'informations dont on disposait jusqu'à récemment sur sa genèse.

5 Cette automatisation des tâches a eu de profondes répercussions sur l'organisation du travail. Des groupes interdisciplinaires perdurant après la guerre ont été créés en rassemblant des ingénieurs, des linguistes, des physiciens et des mathématiciens, comme Alan Turing. D'immenses bureaux ont été ouverts pour y faire travailler des centaines de femmes chargées de préparer les données à entrer sur ces machines et la quarantaine de photos reproduites dans le livre permet de se rendre compte de cette nouvelle division du travail.

6 Par ailleurs, le livre de S. Budiansky nous renseigne sur les liens entre les décisions politiques et militaires. Souvent, les rapports issus des services de cryptoanalyse pouvaient suggérer des déclarations ou des ordres qui risquaient de montrer à l'ennemi que sa méthode de cryptage avait été comprise. Dans ce cas, il est certain que l'ennemi allait améliorer la sécurité de ses transmissions et on risquait de perdre par la suite des informations importantes. S. Budiansky expose ce dilemme à travers de nombreux exemples : le fait que W. Churchill avait eu connaissance dès août 1941 du sort réservé aux juifs sur le front Est (le rapport qui lui fut transmis faisait état de dizaines de milliers d'exécutions sommaires, « *savage intimidation if not ultimate extermination* »), l'anticipation de l'attaque de Pearl Arbor, l'attaque sur l'archipel des Midway (et non Hawaii ou les îles Aléoutiennes, en juin 1942), ou encore l'offensive des Ardennes menées par les Allemands en décembre 1944.

7 La coopération parfois difficile entre Britanniques et Américains et les rivalités entre l'armée de l'air et la Marine eurent aussi pour effet de compliquer l'utilisation des rapports. Au total, S. Budiansky offre une vision mesurée de l'importance de la cryptologie, rappelant que la reconnaissance aérienne et les services de renseignements jouèrent un rôle complémentaire. Ce livre est à recommander à toute personne intéressée par l'histoire de la Seconde Guerre mondiale.

AUTEUR

JÉRÔME SEGAL

Maître de conférences à l'IUFM de Paris