An Inventory of Early Inter-Allied Enigma Cooperation

Marek Grajek
Freelance cryptography consultant and historian
Poland
mjg@interia.eu

Abstract

Shortcomings in the earliest reports coming from the wartime work at Bletchley Park resulted in a slightly distorted picture of the early inter-Allied cooperation in cryptology. The ultimate evidence of the Polish contribution to the success over Enigma, a report passed on to the British and French participants of the meeting in Pyry in July 1939, remains unavailable to historians.
Some files declassified in 2015 by the French intelligence service contain a document representing most probably an abridged and rewritten version of the Pyry report. This paper offers a preliminary analysis of this document.

1 Introduction

Although some attempts to coordinate the British, French and Polish efforts aimed at breaking the Enigma ciphers had been undertaken earlier, the conference at Pyry on 24-27 July 1939 marked the effective start of the inter-Allied cooperation in that field. The general nature of the reports from the Pyry meeting, as known so far, does not allow the precise assessment of the contribution of the countries participating in the conference in unravelling the secret of Enigma at that early stage of work.

Both cryptographers and historians have been aware for a long time of the existence of a definitive source of information regarding the Pyry conference and early work on Enigma. Before the chiefs of Polish intelligence service authorised the invitation of the British and French codebreaking services to Warsaw, they instructed the Cipher Bureau to prepare a detailed report presenting the complete Polish knowledge about, and experience with, the Enigma machine and its ciphers. Copies of that report were passed on to the British and French guests during the Pyry meeting. British post-WWII reports (Alexander, 1945; Mahon, 1945; Millner-Barry et al., 1945) contain references to the report indicating that it was available at Bletchley Park in 1945. Unfortunately this document is lost or at least has not been declassified so far and remains unavailable to historians.

This author believes that he has identified a document representing an edited, albeit a slightly later and abridged version, of the original Pyry report. The document found is potentially even more valuable than the original report, covering events up till the fall of France in June 1940. It may be regarded as an inventory of the early inter-Allied cooperation in the struggle against the Enigma ciphers. This paper presents early findings regarding this document.

2 Historical context

Since their first meeting in Paris, in January 1939, chiefs of the codebreaking services of the three countries, France, Great Britain, and Poland, knew that finding a common language was not going to be easy. In the literal sense of the word they could hardly find a way to communicate, before they agreed to use the language of their common cryptologic adversary – German. They did not know at that stage that they were coming to the table bearing different levels of knowledge regarding Enigma, experience and probably – different instructions and goals. The tension around the table was almost palpable, in spite of Bertrand's efforts to integrate the group using the services of the best restaurants in Paris. In those circumstances, it is not surprising that the meeting's only measurable result was a decision to convey further meetings, once any of the parties had news to communicate.

That moment arrived sooner than expected; in July invitation from Warsaw arrived, declaring that 'il y a du nouveau'. But when the codebreakers arrived in Warsaw on July 24th they had to switch back to German again, as the document they were discussing was in that language. Mahon (1945, p. 13) stated in his post-war report that "(n)early all the early work on German Naval Enigma was done by Polish cryptographers who handed over the details of their very considerable achievements just before the outbreak of war", and added that "the Poles devised a new method which is of considerable interest. Their account of this system, written in stilted German, still exists and makes amusing reading for anyone who has dealt with machines" (Mahon, 1945, p. 13).

British post-war reports were compiled by G.C.&C.S. section heads, who had no first-hand knowledge of events of 1939. In fact in 1945 no participant of the Pyry conference remained at Bletchley Park. Dilly Knox had passed away in February 1943; Alastair Denniston had been sacked from his position in February 1942 and exiled to the diplomatic section. Mahon admits having gained most of his knowledge about the early attacks at Enigma from Alan Turing; but Turing had neither participated in the Pyry conference, nor was he known to be an effective communicator. Under the circumstances as described, it is natural that post-war reports are full of unanswered questions and presumptions of disputable value.

The view of early work on Enigma became even more confused after the British secret services felt obliged in mid-1970s to react to the publication of Bertrand's book. They obviously considered Bertrand's revelation as premature and decided to wrap them up with a shroud of disinformation. Frederick Winterbotham was commissioned to provide a cover version of history: "In 1938 a Polish mechanic had been employed in a factory in Eastern Germany which was making (…) some sort of secret signalling machine. (…) In due course the young Pole was (…) secretly smuggled out under a false passport (…), installed in Paris where (…) he was given a workshop. With the help of a carpenter to look after him, he began to make a wooden mock-up of the machine he had been working on in Germany" (Winterbotham, 1974). Similar versions of this story were later on presented by Cave Brown (1975), Stevenson (1976) and, in more recent times, by Aldrich (2010) and Davies (2008). Their stories have a crucial element in common in attempting to provide a cover for the compromise of Enigma ciphers in the breach of machine's physical security. That reaction is understandable; in 1973, when Bertrand (1973) revealed the Allied success with Enigma ciphers, the Cold War was at full swing and the armies of Warsaw Pact were making extensive use of rotor cipher machines derived from the results of the evolution of Enigma. While we could understand the versions of events presented by Winterbotham, Cave Brown and Stevenson as obvious disinformation, the same information produced in the 21st century represents nothing more than anachronism. On the other hand, however, it illustrates the need for an ultimate proof of the real scope of contributions delivered by the Allied nations to the victory over Enigma. For the author of this paper, this was the main reason to spend several years searching for the document which could provide indisputable evidence.

Until recently this search did not bring encouraging results. Archivists representing major institutions were sceptical. According to their opinions, if the document in question had been written in the German language, the chances are that it had been transferred to the German files immediately after the war, where it has stayed unrecognised up till now or has been entirely lost. However, on 2 December 2015, the French Direction Générale de la Sécurité Extérieure announced the declassification of the set of documents relating to the French role in Enigma breaking and the transfer of those documents to the archives of the Service Historique de la Défence. Preliminary investigation of these documents at Château de Vincennes confirmed that they represented part of the private archive accumulated by the late Gen. Gustave Bertrand over the years of his active service at various units of French intelligence service and seized by his former employer immediately after the General's death at his home at Théoule-sur-Mer.

3 Preliminary analysis of the document

Bertrand's collection represents an extremely interesting object of research for Enigma historians. In this paper we shall focus on just one of its elements; an unsigned and undated typescript described in the inventory as "Technical note in German"[1] (unsigned, 1940a). The document is 61 pages long, contains a title page, a table of contents, and 38 sections. Its title page leaves no doubt as to its contents: "ENIGMA. Abridged presentation of solution

[1] In original: Notice technique en allemande.

methods"[2], and its preface partially reveals the identity of its, otherwise unsigned, authors; "Below we sketch how the Cipher Bureau of the Polish General Staff managed to reconstruct the Enigma model described above, and methods invented to assure prompt deciphering of its messages, in spite of the changes and improvements introduced by the German cipher service to protect their security". A brief mention in one of Lt. Col. Langer's (former head of Polish Cipher Bureau) reports allowed this author not only to place the document in its time-line, but also to understand the circumstances of its creation. After his liberation from the German internment camp, Langer (1945) was commissioned to write a report presenting the circumstances of his team's evacuation from southern France in 1942 and the events that followed. It is in that report that we find a following statement: "At Château des Fouzes, Bertrand requested that a report be prepared presenting the contribution brought by each of three partners to Enigma solution. The report was prepared by Lt. Rejewski and Zygalski. After Bertrand had studied the result he declared that the work must be rewritten from scratch, as reading it in its present form one gets the impression that the contribution of the French was negligible". The declared purpose of the report is consistent with its otherwise somewhat mysterious fragment; Section 38 presents an inventory of contributions of the three countries towards the success over Enigma ciphers (see Figure 1 below).

The analysed document is unsigned; the same report by Langer sheds some light and a bit of doubt on the question of its authorship. According to that report, the document was prepared by Marian Rejewski and Henryk Zygalski. That would point to its creation either in 1941 (during Jerzy Różycki's detachment to Algiers) or in 1942 (after Różycki's death). This author believes that more probable time of its creation was late 1940 or early 1941, when Bertrand was still unable to provide the codebreakers with enough intercepts to keep them engaged. Moreover, should the document have been written in 1942, it would most probably include some references to codebreakers' work at P.C. Cadix. It is also possible that Langer, when writing his report in 1945, had confused the question of the document's attribution. The German reports based on his interrogation in 1944 mention only two mathematicians; it seems probable that Langer's mind adjusted (consciously or unconsciously) to the situation after Różycki's death.

While the scope of the document covers events having taken place between the Pyry conference and the fall of France in June 1940, its basic structure and form, as well as comparison with other documents edited by Marian Rejewski and his colleagues, suggest existence of their common source – presumed to be the Pyry report. The term "abridged" used in the title might suggest existence of a full version of the same document. Working in France, in 1940 or later, at Bertrand's request, it would be natural for the codebreakers to prepare the text in French (at least two members of the team were fluent in that language). However, existence of the German language reference, and economy of labour dictated the preparation of an abridged version of the existing German language document, complementing it with coverage of the recent events and adding elements specifically requested by Bertrand.

While working on the original Pyry report, the codebreakers having full access to their own archive, could, and certainly would have wanted to, demonstrate their mastery of the subject by including as much detail as possible. However, the archive of the Cipher Bureau was lost during its evacuation towards the Romanian border. When the team attempted to continue its work in France, the Poles had to recreate their documentation using their memory as the only reference available. Process was slow and gradual, as can be seen from the effects of its first stage – the so called "Dokument L" (unsigned, 1940b), representing an appendix to Langer's report from the pre-war activity of the Cipher Bureau. "Dokument L" was written during the first half of 1940 and supposedly covers the period 1930-1940 (although its scope ends with the Pyry conference). In spite of its scope similar to the discussed document it counts only 31 pages – about half of the latter.

British reports prepared in 1945 include some details of the Polish pre-war activities, which are otherwise unknown from the available Polish sources. Alexander (1945, p. 18) describes the Polish attack on naval Enigma using the term "Forty Weepy". That term was coined by the

[2] In original: ENIGMA. Kurzgefasste Darstellung der Auflösungsmethoden.

Poles from the representation of numbers used by Kriegsmarine cipher clerks in 1937. The British codebreakers could not have known about that from their own experience, as the system was changed before they focused attention on the naval Enigma. The same report by Alexander names the call sign, AFA, of the German torpedo boat whose signals permitted Polish codebreakers to break the new Enigma procedure adopted by Kriegsmarine in May 1937. None of those details ("Forty Weepy" or AFA) are mentioned in the analysed document (or any other Polish sources) and must have been known to the British codebreakers from the original Pyry report.

The scope of information regarding pre-war efforts of the Polish Cipher Bureau available in the analysed document goes far beyond the limits of the original, Polish sources available so far. On the other hand it does not include some details quoted in the existing British reports. The structure of the document is very similar, even in translation, to the structures of other documents edited by the members of Cipher Bureau team ("Dokument L" or Rejewski's "Memories"), hinting at their common source. All those details considered together permit the positioning of the document as an intermediate link between the fragmentary sources known so far and their common reference – the original Pyry report.

4 Preliminary findings and conclusions

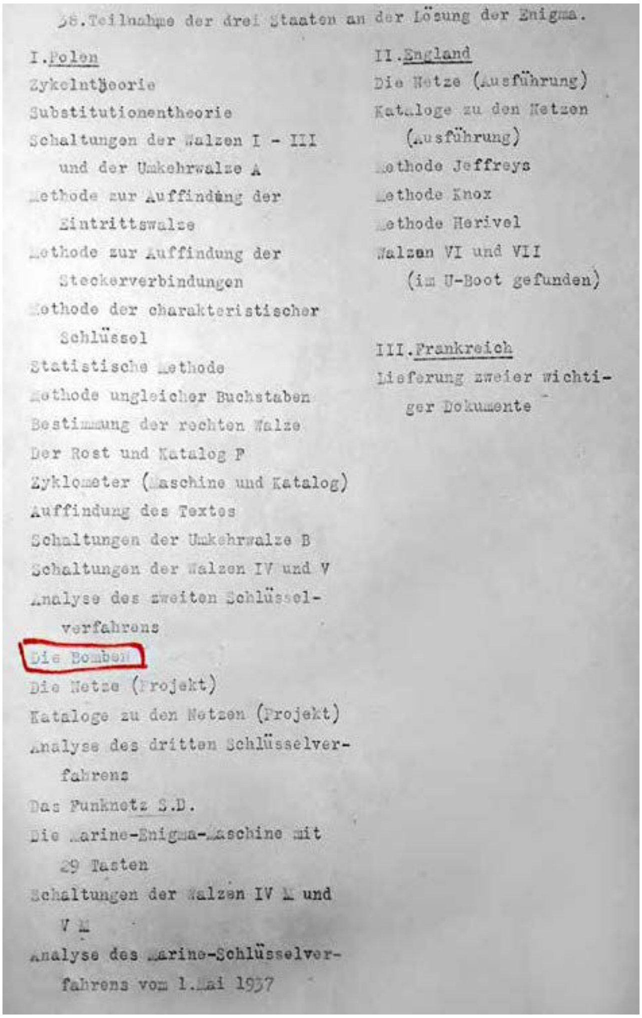
Systematic analysis of this recently found document is far beyond the scope of this paper, although the preface to the edited version (Grajek, 2017) of the report provides its early stage. The document, although obviously not identical to the original Pyry report, represents the best approximation currently available. It has been created by the same team, for the similar purpose and using the same language. It is the first material proof of otherwise obvious fact – the transfer of Enigma secrets by Polish Cipher Bureau to the Allies, which was found in the Allied archives. This author hopes that this information might spark a wider search for its presumed predecessor – the original Pyry report.

Most facts presented in the report are known from other sources, in particular from "Dokument L" and Rejewski's "Memories"; however, in the discussed document they are presented in a more systematic way than in other versions. At least some novel elements deserve special attention. The first one concerns the radio network of the German Sicherheitsdienst (S.D.). Section 34 presents the history of Polish struggle with the S.D. network between its first appearance in October 1937 and a major change on 1 August 1939. Messages in the S.D. network were masked with a 3-letter code before enciphering with Enigma. That did not prevent Polish codebreakers from breaking both the code and the Enigma key and reading the messages up to 31 July 1939.

This statement contradicts the opinion formulated in Dilly Knox's (1939a) report from the Pyry meeting, and repeated since then by numerous sources, that Poles were unable to read Enigma after the change of the indicator structure on 15 September 1938. The statement in Section 27 reinforces this argument indicating that the military key from 25 August 1939, the day of general German mobilization, was the last broken day before the evacuation of the Cipher Bureau from Warsaw.

Section 29 refers to the preparation by Bletchley Park staff of a special catalogue already proposed by the Poles before the outbreak of war. Lack of resources prevented the Polish team from implementing its own idea, but the more resourceful British were able to manufacture the proposed catalogue, which went into history as Jeffreys' sheets. Jeffreys' sheets represented an extension of Zygalski sheets; while the latter identified only the location of a female, the former permitted also to identify the character corresponding to the female ("(…) we had the idea to create catalogues with characters that would correspond to all female cases, (…) now the British (…) put our plans into practice").

Section 30 offers an update to the history of the Herivel method, which was brilliantly conceived but useless as long as the positions of the turnover notches in rotors IV and V were unknown. Herivel's discovery was complemented by the Polish team, who identified the notch positions in both rotors and communicating them to BP thereby enabling the practical application of the Herivel Tip.



38. Teilnahme der drei Staaten an der Lösung der Enigma.

I. Polen

Zykelntheorie
Substitutionentheorie
Schaltungen der Walzen I - III
und der Umkehrwalze A
Methode zur Auffindung der
Eintrittswalze
Methode zur Auffindung der
Steckerverbindungen
Methode der charakteristischer
Schlüssel
Statistische Methode
Methode ungleicher Buchstaben
Bestimmung der rechten Walze
Der Rost und Katalog F
Zyklometer (Maschine und Katalog)
Auffindung des Textes
Schaltungen der Umkehrwalze B
Schaltungen der Walzen IV und V
Analyse des zweiten Schlüsselverfahrens
Die Bomben
Die Netze (Projekt)
Kataloge zu den Netzen (Projekt)
Analyse des dritten Schlüsselverfahrens
Das Funknetz S.D.
Die Marine-Enigma-Maschine mit
29 Tasten
Schaltungen der Walzen IV M und
V M
Analyse des Marine-Schlüsselverfahrens vom 1. Mai 1937

II. England

Die Netze (Ausführung)
Kataloge zu den Netzen
(Ausführung)
Methode Jeffreys
Methode Knox
Methode Herivel
Walzen VI und VII
(im U-Boot gefunden)

III. Frankreich

Lieferung zweier wichtiger Dokumente

Figure 1: Final section of the analysed document - contributions of the three states to the breaking of Enigma

Section 31 refers to the new Enigma ciphering procedure used from 1 May 1940. We learn that some German cipher clerks started to use it prematurely, on 30 April. The Poles, who managed to break the military key for that day, were able to work out the procedure and communicate its details to Bletchley.

While sections 1–32 have a more or less chronological structure, section 33 is dedicated to the S.D. network, Sections 34–37 break the chronological narration and represent an appendix dedicated to the area only incidentally covered in the reports known so far – the ciphers of the German Kriegsmarine. The story long established among Enigma historians states that while Poles provided the foundations for breaking the Wehrmacht and Luftwaffe ciphers, breaking the Kriegsmarine Enigma represented a purely British adventure. The analysed document presents this question in a new light. The Poles were obviously watching the evolution and breaking the Kriegsmarine ciphers from their non-machine beginnings to the establishment in May 1937 of the system used during the war. The report confirms that they were able to work out the details of the new procedure and, thanks to the German blunder in the transition period, to break enough messages to provide the British codebreakers with the reference material for their own efforts. Alan Turing and his team designed a number of methods (EINS-ing, banburismus) which could assure regular decryption operation once the system is first broken, however they could not advance their practical mastery of the cipher beyond the point reached by the Poles in 1937. Their final success in 1941 was based both on the information provided by the Poles and the documents captured on board the seized German ships.

Section 38 represents an element of the document most appealing to the reader's mind; it offers an enumerative list of elements contributed by the three participants of the cryptologic cooperation until June 1940 (cf. Figure 1 below). While this picture has changed significantly in the later stages of war, there is no doubt that during the first year of this conflict, the Enigma adventure was still heavily dominated by the achievements of the Polish Cipher Bureau team.

Acknowledgements

I would like to express my gratitude to Sir Dermot Turing for providing an important clue, and to Philippe Guillot for assisting my research. I would like to thank also the Internal Security Agency of Republic of Poland for its help in publishing the source version of the document.

References

Aldrich, Richard J. 2010. *GCHQ. The Uncensored Story of Britain's most secret intelligence agency*, Harper Press.

Alexander, C.H.O'D. 1945. *Cryptographic History of Work on the German Naval Enigma*, NA HW 25/1.

Bertrand Gustave. 1973. *ENIGMA ou la plus grande énigme de la guerre 1939-1945*, Librarie Plon, Paris

Cave Brown, Anthony. 1975. *Bodyguard of Lies*, Harper and Row.

Davies, Norman 2008. *Europe at War 1939-1945. No Simple Victory*, Pan Macmillan.

Denniston, A. G., *How News was Brought from Warsaw at the end of July 1939*, NA 25/12

Grajek Marek. 2017. Sztafeta Enigmy. Odnaleziony raport polskich kryptologów, ABW, Centralny Ośrodek Szkolenia ABW, Emów.

Knox, A. D. 1939a. *Letter to A. G. Denniston*, 1939, NA HW 25/12

Knox, A. D. 1939b. *Memorandum*, NA HW 25/12.

Langer, Gwido Karol. 1945. *Sprawozdanie dotyczące ewakuacji Ekspozytury Nr 300*, Instytut Józefa Piłsudskiego w Londynie, 709/133/5.

Mahon, A.P. 1945. *The History of Hut Eight*, NA HW 25/2.

Milner-Barry, Philip Stuart (ed.). 1945. *The History of Hut Six*, NA HW 4/70.

Rejewski, Marian, Zygalski, Henryk. 1940. *ENIGMA 1930-1940. Metoda i historia rozwiązania niemieckiego szyfru maszynowego (w zarysie).*

Rejewski Marian. 1967. *Memories of my work at the Cipher Bureau of the General Staff Second Department 1930-1945*, Adam Mickiewicz University Press, Poznań 2013

Stevenson, William. 1976. *A Man Called Intrepid*, Skyhorse Publishing, New York.

Unsigned. 1940a. *Notice technique en allemande [sans date]*, SHD DE2016 ZB25 6, Dossier 281.

Unsigned. 1940b. *Dokument L, appendix to Lt. Col. Langer's report on Polish Cipher Bureau's pre-war activities*, Instytut Józefa Piłsudskiego w Londynie, 709/133/5.

Winterbotham, Frederic. 1974. *The Ultra Secret*, Weidenfeld and Nicolson, London