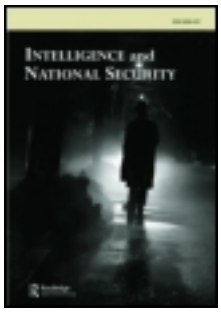

Intelligence and National Security
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/fint20

From Polish Bomba to british Bombe: The birth of ultra

Gordon Welchman [a b]
[a] Lecturer in Mathematics, Cambridge University,
[b] Fellow of Sidney Sussex College,

Available online: 02 Jan 2008

To cite this article: Gordon Welchman (1986): From Polish Bomba to british Bombe: The birth of ultra, Intelligence and National Security, 1:1, 71-110

To link to this article: http://dx.doi.org/10.1080/02684528608431842

From Polish Bomba to British Bombe: The Birth of Ultra

GORDON WELCHMAN

I

THE POLES, THE BRITISH AND THE FRENCH

Until just before the Second World War a small Polish team of three mathematician-cryptologists, headed by the brilliant Marian Rejewski, had been happily breaking the German military cipher machine, the Enigma, for many years. A small British team under the First World War cryptanalyst, Dilly Knox, was near to success, but was foiled by failure to make a guess which, in retrospect, seems an obvious one. The French cryptanalysts do not appear to have tried, but Captain Gustave Bertrand, involved in French espionage, achieved a coup without which the Polish breaks and the subsequent British successes might never have been achieved.

The Poles kept their secret to themselves until July 1939 when, with the German invasion of their country imminent, they gave all their knowledge, as well as working replicas of the Enigma machine, to the French and British. In England, at Bletchley Park, we were quick to exploit the golden opportunity that the Poles had handed us. In France Bertrand established an organisation near Paris, code-named Bruno, at which Marian Rejewski and his associates Henryk Zygalski and Jerzy Rozycki, having escaped from Poland, continued to work on Enigma. There was collaboration between Bletchley and Bruno until the German advance on Paris forced an evacuation.

Ultra intelligence, based on decodes of the Enigma traffic of the German army and air force, was born early in 1940. Its heyday started after the battles of El Alamein and Stalingrad in the autumn of 1942 and the Allied landing in North Africa in November 1942. By that time the Allies had become strong enough to take advantage of this extraordinarily prolific source of intelligence, and a satisfactory means of sending Ultra information to commanders in the field had been developed.

As early as 1941 and 1942 Rejewski wrote reports in Polish on the prewar breaking of the Enigma cipher. More than 30 years later, in 1973, Bertrand, infuriated by the publication of a completely erroneous

account, decided to break silence. He published a book revealing that Enigma had been broken during the war.[1] This book, however, was not reviewed in any important periodical and sold very badly. The publication of Winterbotham's book, *The Ultra Secret*,[2] in 1974 was a very different story. Awareness of the major contribution that Ultra had made to Allied victory spread rapidly around the world. It is ironical that the editor of a French translation of Winterbotham's book had no idea of the existence of Bertrand's publication.

Since 1974 a great deal has been written about Ultra and many misconceptions have arisen. I myself, as author of *The Hut Six Story*,[3] have given rise to some of these. When I arrived at Bletchley Park in September 1939, Dilly Knox told me nothing about how the Poles had acquired the knowledge that they passed on to us. I had not even appreciated our debt to Rejewski until Professor Stengers sent me a copy of his paper in the February 1981 issue of *L'Histoire*.[4] With my book going to press a few months later, all I could do was make minor additions in the text and pay tribute to Rejewski in the dedication. Although Jozef Garlinski's book *The Enigma War*[5] was published in the USA in 1980, I did not hear of it in time to take advantage of the appendix by Colonel Tadeusz Lisicki, which contains an account of Rejewski's achievements.

The January 1982 issue of *Cryptologia* contained a translation of an article by Rejewski himself,[6] together with other information about his work. The April 1982 issue reviewed another article by Rejewski that had been published in *The Annals of the History of Computing*.[7] Two years later, an article by Professor Jean Stengers, 'Enigma, The French, the Poles and the British, 1931–1940' was published in England as part of *The Missing Dimension*, edited by Christopher Andrew and David Dilks.[8] Another book published in 1984 was *Enigma* by Wladyslaw Kozaczuk, edited and translated by Christopher Kasparek,[9] which appears to be an updated version of a book published in Polish in 1979.[10] It contains, as appendices, copies of all but one of the Rejewski articles that appeared in *Cryptologia*. Its last appendix contains many lengthy quotations from my book, *The Hut Six Story*.

The time has come to deal with many misconceptions that have arisen in these and other writings; particularly in Appendix 1 of Volume 1 of the official history of *British Intelligence in the Second World War*.[11] For example, a careful study of Rejewski's writings shows that the 'Bomba' was not as important as it has been made out to be. It had its brief day of glory, but was already ineffective when the Poles got us off to a flying start by telling us their secrets in July 1939. It would have been of no use to us, as will become apparent after I have discussed Rejewski's brilliant cryptanalytical work. Its name was given to it by Jerzy Rozycki because the idea for the machine came to Rejewski while the three of them were

together and happened to be eating a very popular ice cream, known as a *bomba*, plural *bomby*.

II

THE CRITICAL SIX MONTHS: AUGUST 1939 TO JANUARY 1940

Towards the end of 1983 Andrew Hodges' fascinating book *Alan Turing – The Enigma*[12] reminded me of the early days at Bletchley Park, when Turing and I, with strong support from Edward Travis, then deputy head of GCHQ, were laying the foundations for Ultra. Until I read Hodges' book I did not know that Turing, while at Princeton before the war, had become interested in the use of machines for cryptanalysis. On his return to England he had made contact with Alastair Denniston's GC & CS and was working on Enigma with Dilly Knox, Peter Twinn and Tony Kendrick before the Poles revealed their secrets at Pyry.

The vital secret was the Enigma machine, of which the Poles gave us a replica. The Poles told Knox about the methodology that they had developed and the machines they had built, namely the bomba and the cyclometer. The most important method at that time had been invented by Zygalski and involved the use of large numbers of perforated sheets.

Although I have no firm information on what happened immediately after Pyry, it seems that Knox, Twinn and Kendrick must have set in motion the manufacture of perforated sheets early in August. Turing, probably in consultation with the others, developed several of the new ideas that were involved in the British bombe. Travis made arrangements for the manufacture of the bombe by British Tabulating Machine Company (BTM).

When I turned up at Bletchley at the outbreak of war in September 1939, I was sent along to join Dilly in the Cottage, but he soon sent me off to another building, the School, to work on call signs and discriminants. All I knew at this point was that the Poles had given us an Enigma machine, how it worked, and what enciphering procedures were then in use. I was not even told about the Zygalski sheets or about plans for the bombe. I knew nothing of the clever ways in which Rejewski, Zygalski and Rozycki had taken advantage of the weaknesses of earlier procedures.

As was explained in *The Hut Six Story*, my banishment from the Cottage to work on call signs and discriminants associated with intercepted Enigma messages proved extremely fortunate. In addition to masses of meaningless enciphered texts I was given a small number of decoded German Enigma messages. What happened then is summarised on pages 37 and 38 of my book as follows:

> Previously I suppose I had absorbed the common view that crypt-

> analysis was a matter of dealing with individual messages, of solving intricate puzzles, and of working in a secluded backroom with little contact with the outside world. As I studied that first collection of decodes, however, I began to see, somewhat dimly, that I was involved in something very different. We were dealing with an entire communications system that would serve the needs of the German ground and air forces. The call signs came alive as representing elements of those forces, whose commanders at various echelons would have to send messages to each other. The use of different keys for different purposes, which was known to be the reason for the discriminants, suggested different command structures for the various aspects of military operations.

Much to the disgust of Dilly Knox I soon thought independently of the principle of the Zygalski sheets. Only then did I discover that the sheets were already being manufactured in the Cottage under the direction of John Jeffreys. I then realised that we were almost certainly going to be able to break a good deal of the Enigma traffic and also that, to exploit this great opportunity, we would need the well co-ordinated efforts of several specialised organisations, including the radio interception station at Chatham, with which I had already established close contact. We were faced with an unprecedented situation, quite unlike the cryptanalysts of the old days when messages were broken one by one. If we could discover a 'daily key' which told German operators how to set up their Enigmas, we would be able to decode all messages using that key. Each of several daily keys was valid for 24 hours, and even in the autumn of 1939, when no military operations were in progress, we were intercepting hundreds of messages each day.

No one else seemed to be doing anything about this potential gold mine, so I drew up a comprehensive plan which called for the close co-ordination of radio interception, analysis of intercepted messages, breaking Enigma keys by means of the perforated sheets, decoding messages on the broken keys, and extracting intelligence from the decodes. Travis immediately saw the urgent need to get moving. He won high-level approval for my plan and we were able to start recruiting the high-quality staff that would be needed.[13]

Even now, with all the interest that has been shown in its achievements, there is little if any recognition of the fact that, if Travis and I had not started the build-up of the Hut 6 organisation before the end of 1939, Ultra intelligence might never have come to bloom. For in May 1940, soon after Hitler invaded France, a simple change in enciphering procedure completely defeated the Polish method of using perforated sheets to break Enigma keys. By that time, fortunately, we had built up a strong

team of young new-style cryptanalysts with the necessary supporting activities. They managed to hang on by their eyebrows, or rather by taking advantage of German errors, until the first British bombes arrived many months later.

This team, with its support, would not have been in place in May 1940 if we had not developed what was essentially a radically new production-oriented approach to machine cryptanalysis on a scale that Polish resources could not have achieved. Without the confident expectation and early demonstration of success we would not have been able to win high-level support for the major expansions of staff and facilities that were to prove so necessary. The early start on the manufacture of the Zygalski sheets, which, never having heard of Zygalski, I called the Jeffreys sheets, was of crucial importance to this early success. Furthermore, if the manufacture of the Turing bombe had not been started in August 1939, our early success would have fizzled out. Surprisingly these startling facts are not brought out in the official history of *British Intelligence in the Second World War*.

A good deal of importance has been attached to the fact that first the Poles and then the British brought in mathematicians to work on Enigma. Like Rejewski and Turing, I was a mathematician but, whereas they were both at home with deep problems of mathematical analysis, my principal interest lay in a descriptive approach to algebraic geometry, now out of fashion. However, soon after reinventing the Zygalski sheets, I came up with an abstract idea – the principle of the diagonal board – which greatly increased the power of the Turing bombe. My wartime associate, Pat Bayly,[14] maintains that this idea can be attributed to my pre-war habit of thinking in abstract multi-dimensional space.

III

THE FIRST TWO YEARS: AUGUST 1939–JULY 1941

We will be concerned with three of the many wooden huts that were built to house the activities of GCHQ, numbers 3, 6 and 8. The organisations that started in these huts were known throughout the war as Hut 3, Hut 6 and Hut 8, even after they all moved to a new brick building known as Block D.

Thanks to the flying start that the Poles gave us at Pyry and to the Bletchley Park initiatives of the first six months, we were able to build up a round-the-clock activity in Hut 6 that would support the breaks that were expected once the Jeffreys sheets became available.

For reasons that I will explain later I now believe that a set of the Jeffreys sheets was taken to the Poles at Bruno by Alan Turing on 17

January 1940, that Jeffreys moved from the Cottage to Hut 6 at about the same time, and that intermittent breaking started immediately both at Bletchley and at Bruno. Three members of the Foreign Office staff were assigned to handle the decodes and the intelligence organisation, Hut 3, came into existence.

When Hut 6 began to break with fair regularity, Commander Ellingworth, in charge of the intercept station at Chatham, was brought into the secret. He visited Hut 6, witnessed the breaking process, and talked to John Colman who was already operating our intercept control room round the clock. As a result of this visit the collaboration by telephone between Colman's duty officers and those at Chatham became firmly established. Incidentally the task of Colman's party was co-ordination rather than control, an important distinction.

At the start Jeffreys and his Machine Room handled the process of breaking, while I was concerned with the overall development and co-ordination of the necessary supporting activities. I did not become involved in the breaking until May 1940, when the sheets suddenly became useless. As will become apparent when I discuss Rejewski's work in part V, all the pre-war achievements of the Poles depended on the double encipherment of the wheel setting used to encipher and decipher the text of a message. Soon after they invaded France, the Germans abandoned this double encipherment. Hut 6 was on its own from then on.

We were saved from complete disaster by a form of operator carelessness known as Cillis and by an idea that had occurred to a new recruit, John Herivel, and had become known as the 'Herivel Tip'. The Cillis had been studied in the Cottage for some time. The form of operator laziness that provided the Herivel tip became sufficiently prevalent after the invasion of France, just when we needed it. The combination of these two German errors kept us in business and enabled us to study the decodes and be ready with cribs (accurate guesses at sections of clear text) when the bombes arrived many months later.[15]

Thanks to the success of the perforated sheets during their brief period of glory, the potential value of our ability to read Enigma traffic had been recognised. The Directors of Intelligence of the British army and the Royal Air Force had made it possible for the co-ordination of interception, traffic analysis, cryptanalysis and intelligence to be centralised at Bletchley Park. As I will endeavour to show in part VII, this was one of many things that really mattered.

The handling of naval intelligence derived from Enigma traffic of the German navy is another matter. Hut 8 was established to deal with naval Enigma, and Turing played a key role. But it was a tougher problem than that facing Hut 6. A capture was needed, and this was not achieved until March of 1941. I do not propose to say anything about this except to

remark that the early success of Hut 6 won support for the development of the bombes on which the breaking of naval Enigmas would depend. The term 'Ultra', although originally coined by Winterbotham to describe intelligence derived from Hut 6 decodes, has been applied to information from other cryptanalytical sources, including Hut 8. For this reason I introduced the term 'Hut 6 Ultra'.

In September and October of 1940 we learned from Hut 6 decodes that Hitler had abandoned his plans for the invasion of England and that German forces were leaving France. It became clear that the area of operations of the German armies was going to spread into the Balkans and through Italy into Africa. This suggested that not only Hut 6 itself, but all its related activities as well, would need considerable expansion. Again I made a case to Travis and he got things moving. We got the additional capabilities that we needed for the crucial developments of March, April and May of 1941, when the Germans became active in the Balkans and in Africa. The RAF opened their big intercept station at Chicksands, a little to the east of Bletchley. The army station at Chatham moved to Beaumanor, a country estate in Leicestershire, some 50 miles north of Bletchley, where there was enough space for the large aerials needed to pull in distant radio signals.

Both Hut 6 and Hut 3 had begun a major expansion in the first half of 1941. Harold Fletcher, who arrived in August 1941 and was to be the principal administrator of Hut 6 and the bombes, found a well established organisation that was running smoothly. At that time we already had eight to twelve bombes. Thus, at the end of the second year, we had come a long way. The organisation that we had developed would stand up to the increasing complexity of our problems during the remaining four years of the war.

What had been achieved at Bletchley was to have many surprising ramifications. For example, in the second volume of *British Intelligence in the Second World War* Hinsley comments on the desert campaign from May to October 1942, from the lull before Rommel's attack at Gazala to his defeat in the second battle of El Alamein. It was thanks to Ultra, Hinsley says, that the importance of intelligence came to be recognised. At the start of the Gazala battles there was no adequate means of using Y intelligence, but this defect was spotted. Within two weeks, Army Y was fully integrated into the operational intelligence process at Eighth Army Headquarters. Thereafter it produced an extremely valuable flow of tactical intelligence about even the smaller enemy units. In the opinion of the British officer who was to become the head of Eighth Army's operational intelligence, Ultra put intelligence on the map in the Western Desert, but in battle the Army Y service was usually more valuable than Ultra.

Experience gained by the British intelligence community during the first two years was to have an effect on the war in the Pacific. As a result of his many personal contacts with Allied field commanders of the Second World War, Ronald Lewin in his *Ultra Goes to War*[16] stresses the importance of the 'Special Liaison Units' that were developed by Winterbotham to guide the use of Ultra intelligence in the field. The timely selection and training of officers for these units proved to be of the utmost importance. In his *American Magic*[17] Lewin remarks that, before the Japanese attack on Pearl Harbor on 7 December 1941, the Americans were ill-prepared for the problems of handling wartime intelligence, but in January 1942 Alfred McCormack of the New York Bar was assigned by Henry Stimson, the Secretary of War, to look into the matter. His early recommendations resulted in the birth of an intelligence organisation which, in its selection of personnel and its independent status was somewhat similar to Bletchley's Hut 3. Later, during a visit to Bletchley, McCormack was impressed by the well established organisation of SLUs. To build up a similar organisation of 'Special Branch Officers' he promptly recruited what he termed 'imaginative persons of first class ability', who would be attached to all major commands. Lewin's discussions with American field commanders showed that the value of these Special Branch Officers was well recognised everywhere except, apparently, by MacArthur.

Another event that was to be of importance to the Americans as well as to the British should be mentioned here. Before America entered the war, Alastair Denniston, who was head of Bletchley Park during the first two years, visited William Friedman, the chief cryptologist of the US army. One of Friedman's assistants, Frank Rowlett, who played a major role both in the breaking of the Japanese Magic Cipher machine and in the development of an American cipher machine, remembers the visit well. He and Friedman very much admired Denniston both as a person and as an outstanding cryptologist. Rowlett says that the impression Denniston made on the US Army's cryptological organisation undoubtedly helped to establish the close relations with Bletchley Park that were to develop later.

IV

CAUSES OF CONFUSION

Appendices B to E of Wladyslaw Kozaczuk's book, *Enigma*, are based on Marian Rejewski's own accounts of what happened in Poland before the war. These accounts are very clear, and they ring true. They are based on personal recollections that were written down in 1941 and 1942, when Rejewski's memory was still fresh. But few people have taken the trouble

to understand them and as a result misconceptions have arisen. Too much attention has been paid to the statements of his superiors who, though making major contributions in other ways, were never in close contact with Rejewski's cryptanalytical work, which started in 1932.

The superiors were Colonel Stefan Mayer, chief of the intelligence department of the Polish General Staff, Colonel Gwido Langer, head of the Polish Cipher Bureau and Maksymilian Ciezki, head of the German section in the Cipher Bureau. According to Rejewski, Ciezki would come to see him once a day, Langer very seldom, and Mayer once or maybe twice during the whole period from 1932 to 1939.[18]

Kozaczuk's Appendix F, written by Christopher Kasparek and Richard Woytak, is entitled 'Polish and British Methods of Solving Enigma'. Referring to my book, *The Hut Six Story*, the first page contains the statement:

> It is disconcerting to find such a cock-and-bull story repeated with approval in Welchman's otherwise sober and valuable book when so much documentation regarding Polish mastery of Enigma has been published in English.

What seems to me 'disconcerting' is that Kasparek and Woytak, who should have been familiar with the 'documentation', arrived at such a misconception. They should have known that Rejewski's determination of the wiring of the two new wheels (the subject matter of the 'story') was the result of an extraordinary German error. As I said,[19] the article by Jean Stengers did not explain how the wiring became known to Rejewski. Nor did Lisicki's appendix to Garlinski's book *The Enigma War*, published in American in 1980. The true explanation was made known in two articles by Rejewski, first published in English in 1981 and 1982 and reissued as Appendices D and E of Kozaczuk's book, but these were not available to me until after my book went to press in mid-August 1981. I believe that any cryptanalyst who cares to study the matter will agree that a recovery of the wiring of the two new wheels by pure cryptanalysis (without a compromise or a major German blunder) was hard to believe and that it was logical for me to think that the Poles had probably pulled off a capture without the Germans knowing that they had done so.[20] Indeed this is exactly what the British did later on in order to break into the German naval Enigma.[21]

In a review for the *Journal of the U.S. Army War College*, Professor Cipher Deavours, Professor of Mathematics at Kean College, New Jersey, and an editor of *Cryptologia*, says that the Kozaczuk book contains valuable historical lessons for today and is well worth reading. He also says:

> The book's chief flaw consists of its notably anti-British approach. In particular Welchman (whose book is quoted at excessive length) comes in for a lot of undeserved criticism. It is the thesis of the book that 'virtually all major cryptologic techniques that the British used to break Enigma in World War II had been thought of by the Poles earlier'. This statement is simply not true.
>
> Without the Polish work, the British would likely never have gotten started in the first place, but once they did get started, British codebreaking was as dazzling as the earlier Polish accomplishments. The British bombes were in no way related to or derived from the earlier Polish bomby, nor were Polish methods of cryptanalysis particularly useful after the Germans changed to a better message keying system in May 1940.

In fairness I must say that Kozaczuk and his associates had good reason to be resentful of the way British authorities have belittled the Polish contributions to Allied success, on the battlefield as well as in the field of cryptanalysis. But it is unfortunate that they quoted so extensively from *The Hut Six Story* without any reference to me. This has added to the confusion because their Appendix F has repeated, and perhaps given additional credence to, many of my errors (as well as introducing many errors of their own).

To deal with the many misconceptions of Rejewski's brilliant work I will give a summary of what actually happened, based on Rejewski's own statements. Before I do that, however, it should be pointed out that a good deal of confusion has arisen because the relevant information has become available in dribs and drabs. (Some of it is still withheld by the British authorities.) This point is brought out in the chronological list of references at the end of this article. For example, Johnson's *The Secret War* and Hinsley's Appendix 1 to Volume 1 (references 11 and 15), both of which are full of mis-statements, were written before my book (reference 26) came out. Other authors, e.g. Lewin, Jones and Calvocoressi (references 9, 12 and 18) made fewer mistakes. I myself, having been told nothing by Dilly Knox and not having seen the Rejewski writings, was often reduced to guessing. I did try, however, to distinguish between my own direct experience and what seemed probable. My 'approval' of the 'cock-and-bull story' was the statement: 'I am inclined to believe that something of the sort must have occurred.'

Another major source of confusion is the different terminologies that have been used by the many authors who have written about Enigma. I will try to sort things out by comparing my terminology with that used by Rejewski. A good starting point is Figure 3.6 on page 50 of my book, which shows the electrical connections between lampboard, keyboard,

steckerboard and scrambler of the German military Enigma. This gives a more detailed representation of the steckerboard than Rejewski's Figures D–4 and E–3.[22] Note that I use the term 'wheel', while Rejewski uses 'drum' in D–4 and 'rotor' in E–3. I use letters U, L, M, R to represent the four wheels (*Umkehrwaltze*, Left, Middle, Right) of what I call the scrambler unit. Rejewski uses letters R, L, M, N (R for Reversing) and replaces my in-out scrambler terminals by another drum or rotor, called H in D–4 and E (for Entry) in E–3. The two sides of a wheel, drum or rotor are shown in D–3.[23]

In comparing my Figure 3.6 with Rejewski's D–4 and E–3 we run immediately into an important difference of attitude. In all my work on Enigma I knew, because the Poles had told us, that the lower stecker terminals A, B, C, ... Z were connected to scrambler in-out terminals A, B, C, ... Z. This is represented in my diagram by a 26-way connector cable. It never occurred to me to worry about the possibility that the Germans might have introduced yet another permutation at this point. This possibility was very much in Rejewski's mind, and is allowed for in his diagrams by the entry rotor, E of his Figure E–3, shown as drum H in Figure D–4. Knox too had been very much concerned about this possibility.

A minor cause of confusion is that I reserve the word 'drum' to mean one of the rotating units in the double-ended scramblers of Doc Keen's engineering design of the British bombe.[24] There was no Polish equivalent.

Further confusion is caused by different usages of the words 'key' and 'setting'. The keyboard of an Enigma has keys, which I call 'letter keys' to distinguish them from machine keys. In my description of the Enigma,[25] I use the word 'key' to mean the basic set-up of the machine, consisting of the wheel order (*Walzenlage* in the German instruction manual), the settings of the alphabet rings on each wheel (*Ringstellung*) and the cross pluggings on the steckerboard, or 'stecker' (*Steckerverbindung*). Rejewski uses the term 'daily key', which I will adopt here.

At this point I can remove a cause of confusion by introducing the term 'crypto net' to mean a group of units who are issued with the same daily key so that they can communicate with each other. The German radio nets are something else.[26] A radio net could carry encrypted messages of several crypto nets, while a crypto net could use several radio nets. It is extraordinary that these two simple facts have been so little recognised.

So a daily key was issued to members of a crypto net. Discriminants (*Kenngruppen*) were used in the preambles of messages to indicate which crypto net was involved.

I used the term 'machine setting' to mean the positions of the three wheels in an Enigma Scrambler that is already set up in accordance with

the daily key of a crypto net.[27] The encoding of an individual message involved two machine settings:

1. A 'text setting' at which encipherment would start
2. An 'indicator setting' (*Grundstellung*) used to encipher the text setting.

Rejewski calls the text setting a 'key', or 'message key'. He calls the indicator setting the 'basic position'. I will stick to my terminology here.

When I came into the picture in September 1939 I was told how the Germans were using their Enigma at that time. The daily keys for a month were issued to all units of a crypto net. Individual messages were enciphered at text settings chosen by the originating operator. These text settings were enciphered twice at an indicator setting also chosen by the operator. The indicator setting was transmitted in the preamble of the message, and the double enciphered indicator setting, which I called the 'indicator', was transmitted as the first six letters of the enciphered text. The receiving operator, with his machine set up to the same daily key would set his wheels to the indicator setting, decipher the indicator, and so obtain the text setting repeated twice. He would then set his wheels to this text setting and decipher the message.

Let me reiterate that Dilly Knox never told me about Rejewski's work, which I will describe in part V. I and the people who joined me in Hut 6 knew that the Poles had given us a replica of the Enigma, and we soon had modified Typex machines that operated like German military Enigma machines. We knew Zygalski's principle of perforated sheets. We knew the purpose of the discriminants and the way in which the units of a German crypto net would set up their Enigmas to a daily key. And we knew the indicating procedure used at that time for the encipherment and decipherment of individual messages. That was all! But it was enough. Knowledge of the other methods that had been used by the Poles would not have helped us. What really mattered was the machine itself and the stimulus that came from knowing that the Enigma traffic could be broken.

V

REJEWSKI'S BRILLIANT CRYPTANALYSIS

Six Successive Periods

At the end of his recent article Stengers remarks:

> What the Poles themselves did was the result, primarily, of Rejewski's creative spirit. But Rejewski himself could have remained impotent without the Asche documents, and the Asche

> documents were just a bit of luck. A bit of luck and history is changed.

In my chapter, 'A Comedy of Errors', I discuss the principal German errors that led to our success and the simple ways in which we could have been defeated. I concluded with the remark that 'We were lucky'.[28]

Rejewski and his two colleagues had different problems but similar luck. At one point[29] he remarks that a German slip-up (mixing plain text with code) made it possible to break into the Enigma traffic of the *Sicherheitsdienst* or SD, an achievement that, combined with another German error, led to the recovery of the wiring of wheels IV and V. He also remarks that the Germans would have been better off if they had not enciphered their text settings.

To get rid of misconceptions we must distinguish between the very different situations that existed in six successive periods, as follows:

1. From the turn of 1927/28 to September 1932, when Rejewski was assigned to work on Enigma.
2. The brief period from September 1932 to the turn of 1932/33 during which Rejewski, working in isolation, broke the German military Enigma.
3. The relatively quiet period from early 1933 to the end of 1935, during which Rejewski and his team achieved regular breaks of daily keys.
4. From 1 January 1936 to 15 September 1938, a period during which the work load increased, due in part to the introduction of new crypto nets for which daily keys had to be recovered.
5. The three months from 15 September 1938 to 15 December 1938 during which the Polish team were dealing with a major change in the German indicating procedure.
6. From the German introduction of two new wheels, IV and V, on 15 December 1938 to the Pyry disclosures to the French and British of July 1939.

1. Turn of 1927/28 to September 1932

The interest of the Polish Cipher Bureau in Enigma was aroused at the turn of 1927/28 when, on a Saturday afternoon, a package from the German Reich arrived at the Warsaw Customs Office. According to the accompanying declaration it contained radio equipment. The German firm's representative demanded very strenuously that the package be returned to the Reich even before going through Customs, since it had been shipped by mistake. The customs officials were suspicious and notified the Cipher Bureau, which was interested in new developments of radio equipment. The package could not be returned until after the

weekend, so personnel from the Bureau had plenty of time to investigate. They carefully opened the box and found that it contained a cipher machine. They examined the machine minutely and carefully closed the box again.[30]

Rejewski insists that this Enigma was a commercial model with no steckerboard. The military model had not yet been put into use. Indeed the first machine-enciphered messages did not appear on German military radio nets until 18 July 1928. The importance of the incident lay in the fact that it revealed German interest in the Enigma. The Polish Cipher Bureau bought one of the commercial machines. At the turn of 1928/29 they organised a cryptology course in Poznan for mathematics students who were fluent in German. This proved to be good thinking.

2. September 1932 to the turn of 1932/33

The second period started on 1 September 1932 when three students who had attended this course, Rejewski, Zygalski and Rozyki, were hired to work permanently at the Cipher Bureau in Warsaw. Rejewski was soon separated from his two colleagues, given a separate room, and instructed to study Enigma. (Earlier studies had been abandoned.) The commercial machine was placed at his disposal, but was of no assistance. Each day he was given several dozen messages enciphered on the military machine.

At that time the German method of using their Enigma was very different from that with which Hut 6 was to be faced seven years later. Of the items in the daily key the wheel order was only changed once a quarter and only six pairs of letters were steckered, leaving 14 unsteckered. The indicator setting was specified as another item in the daily key. From 1 January 1936 the wheel order was changed once a month; from 1 October 1936 it was changed daily, and the number of stecker pairs, instead of being fixed at six, began to vary from five to eight. The indicator setting continued to be part of the daily key until 15 September 1938, after which date the indicator setting for each message was chosen by the operator. It was fortunate that Rejewski was set to work before these improvements in procedure were made.

The fact that the Germans continued for so long to use the same indicator setting for all messages on the same daily key, an extraordinary error, was brilliantly exploited by Rejewski. It became apparent to him that the first six letters of each message text, that I call the 'indicator',[31] were obtained by enciphering the three-letter text setting twice at the same indicator setting. In other words, for all messages on the same daily key the six-letter indicators were the result of encipherment at the same sequence of six positions of the Enigma.

Rejewski denotes the letter permutations produced by the Enigma in these six positions by A, B, C, D, E, F. He started by writing the six-letter

indicators of all messages on a daily key underneath each other. All the indicators that had the same first letter also had the same fourth letter, obtained from the first by the product AD of permutations A and D. The same applied to the second and fifth, and to the third and sixth, involving the products BE and CF.

His next move was to have far-reaching results. Starting with any one of the indicators he wrote down the first letter, say d, and next to it the fourth, say v. He then sought out another indicator that had v as its first letter and wrote its fourth letter, say p, next to d and v. Thus, if three indicators were:

d m q v b n
v o n p u y
p u c f m g

he would obtain the sequence:

d v p f

continuing this process he would obtain a cycle of letters such as:

d v p f k x g z y o

which was closed by the fact that, if the first letter of an indicator was o, the fourth would be the starting letter d.

The remaining indicators would give further closed cycles of the permutation AD. The same procedure would be applied to BE and CF, giving three sets of cycles such as:

AD = (dvpfkxgzyo)(eijmunqlht)(bc)(vw)(a)(s)
BE = (blfqveoum)(hipswizrn)(axt)(cyg)(d)(k)
CF = (abvikrigfcqny)(duzrehlxwpsmo)

This simple method of representing the permutations AD, BE and CF, which Rejewski hit on right away, turned out to be of immense importance. He found that the composition of the cycles was different each day. Later on he would call the three sets of cycles the 'characteristics' of the permutations AD, BE and CF.

Rejewski quickly developed a mathematical theory of these characteristics and, by guessing that some German operators might select three identical letters, such as aaa, bbb, for their text settings, he was able to recover the six permutations A, B, C, D, E, F and so determine the text settings of all messages on the same daily key. In fact, without knowing either the internal connections of the wheels or the set up of a daily key, he had broken the indicating system. To form the three complete characteristics of a daily key all he needed was about 60 messages on that key. It sounds incredible, but it happened.

Still working in isolation, Rejewski's next step was to develop a mathematical representation of the working of the Enigma machine. He was hoping that the knowledge of permutations A to F would enable him to work out the wiring of the wheels. He had reduced his problem to a set of six equations involving three unknown permutations, and he was wondering whether they could be solved, when, on 9 December 1932, at just the right moment, he was given four documents. He did not know it at the time, but these documents had been obtained by Bertrand from the German traitor Asche.

The four documents were a *Gebrauchsanweisung* (operating instructions), a *Schlusselanleitung* (keying instructions), a table of daily keys for the month of September 1932, and a table of daily keys for the month of October 1932.

It was extremely fortunate that the two months, September and October, occurred in different quarters, during which different wheel orders were in use. The known daily keys for each month, combined with the equations he had developed, enabled him to work out the internal wiring of the two different wheels that appeared on the right. Finding the connections of the third wheel and the *umkehrwalze* presented him with no great difficulties. For each wheel he was able to determine the correct torsion of the sides with respect to each other and the turn-over positions of the alphabet rings. The establishment of all these details depended on attempts to read several messages. Fortunately each of the two monthly tables of daily keys included a sample plain text and its encipherment at a stated daily key and text setting.

At one point in this recovery process Rejewski had seemed to be near defeat. In formulating his equations he had assumed that the wiring of the entry wheel (equivalent to the connections of the 26-way cable in my Figure 3.6[32]) was known to him. At first he assumed that the connections were the same as those of the commercial Enigma, in which the terminals of the scrambler's input-output ring were connected to the terminals of the keyboard and lamps in the order in which letters appeared on the keyboard, namely:

q w e r t z u i o a s d f g h j k p y x c v b n m l

This assumption, being wrong, was getting him nowhere, when, at the end of December 1932, or perhaps in the first days of January 1933, he wondered whether the Germans might have used the alphabetical sequence a b c ... z instead of the keyboard sequence q w e ... l. This inspired guess proved correct. The very first trial yielded a positive result. Then, from his pencil, as if by magic, began to issue numbers designating the connections of the right-hand wheel.[33]

Now that the wiring was known, the Poles could modify their commercial Enigma to operate like the German military Enigma. At this point Rejewski was allowed to initiate Zygalski and Rozycki so that, using the daily keys supplied by Bertrand, they could decipher messages that had been intercepted during September and October 1932. Rejewski continued to work in isolation on the third part of his task. He had broken the system of enciphering text settings. He had worked out the electrical and mechanical details of the military Enigma. He still had to find a means of recovering daily keys, and this, as he modestly says, was 'hardly easy'. He developed what he called the 'grill' method. It was very laborious, but, combined with the fact, shown up by decodes of September and October 1932, that many plain texts began with the three letters A N X, it was effective. Thus in January 1933 the Poles were in business. They were able to decode current Enigma traffic. What an extraordinary achievement for a period of a little over four months! And what a brilliant one-man triumph for Rejewski!

3. Early 1933 to the end of 1935

When Rejewski reported his success, the Cipher Bureau ordered a series of replicas of the German military Enigma to be built. (Rejewski calls them 'doubles'.) Then five or six young persons were hired to decipher intercepted messages, the keys to which were soon forthcoming. Zygalski and Rozycki were assigned to work permanently with Rejewski.

Day by day the daily keys were recovered by this three-man team. For three years, until the end of 1935, the Germans introduced no essential changes, so time could be devoted to improving methodology. In his mathematical representation Rejewski had used letter Q to denote the permutation produced by the middle wheel, left-hand wheel and *umkehrwaltze*. A catalogue was made of all the possible permutations Q so that, when the early stages of the grill method had determined the setting of the right hand wheel and the permutation Q, reference to the catalogue would at once reveal the settings of the other two wheels. Rozycki worked out a 'clock method' which, in many cases, could determine which wheel was on the right. This became important when changes of wheel order occurred monthly, and then daily, instead of quarterly. At some point German operators were forbidden to use text settings consisting of three identical letters, but they developed other habits which still allowed the Polish team to determine the permutations A to F.

4. 1 January 1936 to 15 September 1938

The fourth period saw two very important developments; the invention of the Cyclometer and the breaking of the SD Enigma traffic. Already, from 1 August 1935, the German air force had created its own crypto net with

its own daily keys. Gradually other military and paramilitary organisations joined in, forming additional crypto nets with their own daily keys. This implied a great increase in the work load of the three-man team. Furthermore, from 1 October 1936, five to eight pairs of stecker were used, which made it difficult to apply Rejewski's grill method. It became necessary to look for other methods.

Thoughts went back to the characteristics that Rejewski had investigated in September 1932. It dawned on the team that, if they could make a complete catalogue of all possible characteristics, the recovery of the three characteristics of a new daily key, achieved as usual by an analysis of indicators, would lead very quickly to the complete recovery of that daily key. The time-consuming demands of the grill method would be avoided.

Rejewski then invented a machine, the Cyclometer, that would permit the construction of this catalogue. It consisted of two Enigma scramblers with the right-hand wheel of the second scrambler displaced three positions with respect to that of the first scrambler. The overall layout is shown in his Figure E–4, the interconnections of the two scramblers in Figure E–5.[34] The cycles of a characteristic always occurred in complementary pairs of equal length. When current was turned on at any letter, all letters in the same cycle and in the complementary cycle would be shown up by lamps.

This is shown in Figure E–5, in which the 'reversing drum' represents the permutation Q, which is assumed to remain unchanged. When a switch puts current into the first (left-hand) scrambler at position 1, it returns at position r, enters the second scrambler at this position and returns at position w and, after going through the second scrambler unit again, returns to the starting position 1. Thus, for the particular setting of the wheels that is being tested, we have two complementary cycles (l,z) and (r,w). Using other switches reveals the other pairs of complementary cycles. The cyclometer had a rheostat because the number of lamps to be lit would vary.

In September 1932 Rejewski obtained three characteristics for the permutations AD, BE and CF involved in the double encipherment of text settings. Now, for each of the six wheel orders and each of the $26 \times 26 \times 26$ possible positions of the first scrambler, the cyclometer would enable him to obtain a characteristic. The cycle lengths of each characteristic would be entered on a card, probably in order of decreasing magnitude, and the $6 \times 26 \times 26 \times 26$ cards so obtained would be arranged as a card index. Once this major task was accomplished, the recovery of a new daily key would be greatly simplified. The first step, as before, would be to accumulate enough intercepted messages on a new daily key to permit the construction of the characteristics of the three permutations AD, BE and CF. These three characteristics would be looked up in the

card index and, as a rule, the break would be completed in 10–20 minutes.[35]

Rejewski does not say how the turn-over problem was handled, but, except in the worst possible case, at least one of the permutations AD, BE, CF would be unaffected by turn-over and this would greatly reduce the labour involved in completing the break.

The Polish team had a severe setback when on 2 November 1937, soon after the card catalogue of characteristics had been completed, the Germans introduced a new *umkehrwaltze*. At about the same time, however, luck smiled on them once again.

In September 1937 a new crypto net had appeared. It was used by the *Sicherheitsdienst*, or SD. The usual methods provided the wheel order, indicator setting and stecker but attempts to complete a break by looking for messages that began with the letters A N X failed. The ring settings could not be determined. This problem arose from the use of a four-letter code to represent the clear text before it was enciphered on the Enigma. But the Germans enciphered the word '*ein*', for which it seems that there was no four-letter code. With perhaps one and a half ounces of luck this was spotted. The Polish team proceeded to break the four-letter code, and the breaking of the SD crypto net became routine.

5. *The three months 15 September 1938 to 15 December 1938*

The change of *umkehrwaltze* on 2 November 1937 was nothing compared with the blow that hit the Polish team in September 1938. Every single technique that they had used until then had depended on the inexplicable German error of using the same indicator setting for the double encipherment of the text settings of all messages using the same daily key. Suddenly, on 15 September 1938, new regulations called for the arbitrary selection by each operator of the indicator setting for each message. The doubly enciphered text setting – the indicator – still appeared as the first six letters of the enciphered text. The chosen indicator setting was included in the preamble.

The response of the Polish team to this change was amazingly rapid. Within a few weeks – Rejewski estimates one or two – they developed ways to realise two new ideas. Furthermore – and this was a real stroke of luck – they could still read traffic on the SD crypto net which had not yet applied the new procedure.

There were two inventions – the 'bomba' by Rejewski and the 'perforated sheets' by Zygalski. Of these the bomba was a development from the cyclometer, which grew out of Rejewski's very early discovery of the characteristics. Its importance has been greatly exaggerated.

Thinking about the characteristics now became focused on whether or not a characteristic contained a pair of single-letter cycles. In the example

that I have quoted from Rejewski, the characteristics of AD and BE do, whereas that of CF does not. When the characteristic of AD does contain single-letter cycles, it is possible for the same letter to turn up in the first and fourth positions of an indicator. Otherwise it is impossible for this to happen. Similarly for BE and CF.

Until I read the Rejewski papers I thought that the term 'female' for an indicator in which the first and fourth, or the second and fifth, or the third and sixth letters were the same, had been introduced at Bletchley Park. It now seems that an equivalent term was introduced by the Poles. I also thought that Turing's ideas for a British bombe must have been based on what he had learned of the Polish bomba. Again I was wrong, because I had no knowledge of what the bomba was designed to do. It is strange that Kasparek and Woytak, with all the evidence available to them, should have endorsed this mistake of mine in Appendix F of Kozaczuk's book.

When the Germans made their operators responsible for selecting the indicator setting for each message, the Poles were no longer able to recover the characteristics, but, for each message with its chosen indicator setting, the occurrence of a female in the indicator would indicate that the corresponding permutation, AD, BE or CF, had a characteristic that contained single-letter cycles. This was the basis of both inventions.

Rejewski says:[36]

> Given sufficiently ample cipher material it may happen that on a given day there will be three messages with keys (indicator settings and indicators in my terminology) such as:
>
> | | | |
> |---|---|---|
> | R T J | W A H | W I K |
> | H P L | R A W | K T W |
> | D Q X | D W J | M W R |

The bomba depended on the assumption that the letter W was unsteckered. It required little engineering development because it was essentially three cyclometers, set to the relative positions at which the females had occurred, and then turned automatically (as opposed to manually in the generation of the catalogue of characteristics) through all possible positions.[37] In each position there would be a simple automatic test of whether (assuming letter W to be unsteckered) the three females could have occurred. Six bomby were quickly built, one for each of the six possible wheel orders. Rejewski says that they worked reasonably well as long as the number of stecker pairs varied from 5 to 8. From 1 January 1939 this number was increased to 7 to 10, and the bomby became ineffective. By the time the British became involved the number of stecker pairs had settled at ten. Thus the idea that the British would have wanted to copy the bomba is sheer nonsense.

Zygalski's invention of a method based on perforated sheets was a different matter.[38] It involved no assumptions that certain letters would be unsteckered, and it was immediately copied by the British after Pyry. Because the indicator setting was now chosen by the operator for each message, the characteristics AD, BE and CF would no longer apply to all messages on the same daily key. It would no longer be possible to recover them. On the other hand the occurrence of a female such as:

K I E S P E S N T (a 1–4 female)

would mean that the AD characteristic associated with the indicator setting K I E must contain a pair of single-letter cycles. The same would apply to the BE and CF characteristics of females such as:

R Y M X W N P W V (a 2–5 female)
L T S V B Y Q G Y (a 3–6 female)

What was needed, therefore, for each wheel order, was a catalogue of indicator settings, whose characteristics contain single-letter cycles, and a means of comparing females appearing on the same daily key with this catalogue. It was found that about 40 per cent of the characteristics, shown up by the cyclometer and recorded in the card index, contained single-letter cycles, and Zygalski found a way of making the comparison.

For each of the six possible wheel orders a paper sheet was used to represent each of the 26 possible positions of the left-hand wheel. On each sheet a large rectangle was divided into 51 × 51 small rectangles. The two sides, the top, and the bottom of the large rectangle were lettered 'a' to 'z', and again 'a' to 'y'. This provided a co-ordinate system in which the little rectangles corresponded to positions of the middle and right-hand wheels. In each small rectangle a hole would be perforated if the characteristic of the corresponding setting of the three wheels contained a single-letter cycle. Each such occurrence would call for as many as four perforations.

Given enough females on the same daily key, it was possible to stack sheets on top of each other in accordance with the indicator settings that had given rise to the females. The number of visible apertures would steadily decrease and any left open would represent ring settings that would permit the females to occur.[39] Note that, because the turn-over notches were on the alphabet rings, it would be known whether a turn-over of the middle wheel would occur between the encipherments of the two identical letters. Consequently any female that would involve a turn-over could be discarded.

It is perhaps of interest to note that, when I thought of the same idea, independently, I knew nothing of Rejewski's characteristics. In my attempted reconstruction of my thinking process at the beginning of my

Chapter 4, I realised, as Step 3, that it was not always possible for the Enigma to produce the same letter pairing in two positions three places apart in its cycle. This is equivalent to saying that a characteristic will not always contain a pair of single-letter cycles. From then on my thinking was probably very similar to Zygalski's.

Rejewski and his team had to do the enormous job of cutting about a thousand apertures in each sheet, and they cut them with razor blades! They needed six series of 26 sheets each for the six possible wheel orders and the 26 possible positions of the left-hand wheel. By 15 December 1938 they had made only two series. On that day the Germans started using two new wheels IV and V, which had been issued to all formations, including the SD.[40] This meant 60 possible wheel orders, calling for 60 series of perforated sheets.

6. 15 December 1938 to July 1939

The quick recovery of the wiring of the two new wheels by cryptanalysis – the achievement that I found hard to believe – was made possible by yet another major German error. The SD crypto net introduced the two new wheels on the appointed date, but it was still using the old system of enciphering text settings, which had been abandoned by all other crypto nets on 15 September 1938. Knowing this, the team found a day on which the right hand wheel was on of the original three and applied Rejewski's original grill method. Then, assuming that the left-hand and middle wheels were a known one and an unknown one, they found the connections of the latter wheel in the same way that Rejewski had found the wiring of the wheel that had not appeared on the right in September or October 1932.

Knowing the wiring of all five wheels, the Poles, still a three-man team, continued to read messages of the SD crypto net.[41] This reading was intermittent because although Rozycki's clock method sometimes revealed which wheel was on the right, the grill method – the only method of breaking still applicable – sometimes failed because from 1 January 1939 the number of stecker pairs had risen from seven to 10.

This increase in the number of stecker pairs would have reduced the effectiveness of the bomba, and in any case limited Polish resources prohibited the construction of 54 new bomby to deal with the additional wheel orders. The preparation of 58 more series of perforated sheets was another virtually insoluble problem. It was only possible to read military messages when the three original wheels happened to be in use in the two combinations covered by the existing perforated sheets. When, on 1 July 1939, the SD crypto net shifted to the new indicating procedure, the old grill method ceased to be effective there too.

This was the situation in July 1939, when the Poles told Alastair

Denniston and Dilly Knox all they knew. What I knew of what happened after my arrival at Bletchley Park at the outbreak of war is outlined in *The Hut Six Story*. I still feel very strongly, as a result of some 20 years of research on today's military problems, that this story contains many valuable lessons that are sadly neglected. But my account has two serious gaps. I still do not know what Dilly Knox achieved before Pyry, or what he was up to in August 1939, assisted by Twinn, Kendrick, Turing, and a few other assistants. Nor have I found it easy to obtain reliable information about the wartime collaboration between Dilly Knox and Rejewski's team when they were operating first at Bruno, near Paris, and later, under the code-name Cadiz, near the coast of Vichy, France. From what I have now learned from Polish writings, it seems to me that the achievements of the brilliant Dilly Knox have been belittled in his own country. Even if his cryptanalytical methods of around 45 years ago still need to be concealed, which I doubt, it seems strange that a broad outline of what he actually achieved, and might well have achieved with a little luck, is still subject to veto by today's Government Communications Headquarters.

VI

DILLY KNOX AND BRUNO

Marian Rejewski formed a very high opinion of Dilly Knox at the meeting in Pyry in July 1939. In a conversation with Woytak he said:

> Just how much Braquenie understood, I don't know; but there is no question that Knox grasped everything very quickly, almost as quick as lightning. It was evident that the British really had been working on Enigma. So they didn't require many explanations. They were specialists of a different kind.[42]

Rejewski also said:

> I have the fullest grounds to believe that the British cryptologists were unable to overcome the difficulties caused by the connections in the entry drum. When the meeting of Polish, French and British cipher bureau representatives took place in July 1939, the first question that the cryptologist Dilwyn Knox asked was: What are the connections in the entry drum?[43]

Like all the statements that Rejewski made from his own personal experience, these two ring true. And they make one wonder whether Dilly had actually thought of all the major Polish ideas and had been held up only by failing to make Rejewski's guess that the permutation of the entry drum might be identity.

It seems to me entirely possible that Dilly went through much the same thought processes as Rejewski and his team. He could certainly have discovered the characteristics, just as Rejewski did, and he could have gone on to break the indicator system. It is said that Bertrand brought some of the Asche documents to England, so Dilly may have received the four that were so helpful to Rejewski. In that case he could have been well on the way to recovering the wheel wirings, but prevented from doing so only by failure to guess the wiring of the entry drum. After the Germans stopped using the same indicator setting for all messages on the same daily key, it is possible that Dilly would have thought of Zygalski's idea of using perforated sheets to provide a catalogue of wheel settings that could produce females. After all, I had the same idea myself, and I had no previous experience of cryptanalysis.

Having female indicators on his mind, Dilly could well have thought of associating two Enigma scramblers set three positions apart, as was done in Rejewski's cyclometer. With Turing around it is quite possible that, before the Pyry conference the idea of mechanising the movement of the two scramblers would have emerged. The Polish bomba was essentially a combination of three mechanised cyclometers, and the idea of driving a set of scramblers automatically through all possible positions is the only feature of the Polish bomba that was used in the British bombe. It is even conceivable that, before Pyry, Turing and Dilly may have begun to think of using a larger battery of scramblers, not just to handle three females with the assumption that the letter involved would be self-steckered but to handle textual cribs with no such assumption. But, of course, the ideas of the perforated sheets and the battery of automatically driven scramblers could not be exploited without a knowledge of the wiring of the Enigma wheels, which was provided by the Poles at Pyry.

The development of the British bombe involved four new ideas, descriptions of which will be found in *The Hut Six Story*:

1. Loops derived from a crib (p.79)
2. The double-ended Enigma scrambler (p.297)
3. The diagonal board (p.304)
4. Taking advantage of the 'filling up' of the test-register (p.301)

In addition the design engineer, Doc Keen, used what I call 'drums' instead of wheels to get greater speed.[44] Lisicki has confirmed that none of these ideas were known to Rejewski. In a letter to me Lisicki said:

> None of the ideas which you listed were Rejewski's. He was happy with the sheets and discarded the idea of improving his bomba. The loops, the double-ended Enigma, the diagonal board, and the filling up of the test register were all British ideas, and Rejewski in his

> letters to me several times mentioned that he had no idea how to mechanize the search for the keys and thought that the British mechanized the sheets, but that would be useless after May 1940. In Bruno he had absolutely no time for creative work. The running of a number of Enigma scramblers was the only idea which the Poles first used and perhaps was born from the Cyklometer.

My suggestions of what Knox may have done before Pyry are pure conjecture, based on Rejewski's feeling that he must have done a lot. Kozaczuk and Kasparek had no right to assert, as they appear to do, that none of the Polish ideas had been thought of by the British. Furthermore, as Deavours says in the review of the Kozaczuk book that I have quoted, their thesis that 'virtually all major cryptologic techniques that the British used to break Enigma in World War II had been thought of and used by the Poles earlier' is simply not true.

On the other hand the Poles did give us the wirings of the Enigma wheels, and I still maintain that, had they not done so, British breaking of the Enigma might well have failed to get off the ground. Indeed, it is deplorable that the official history of *British Intelligence in the Second World War* has tried to establish that the Polish contribution had little effect. More about this in the next section.

One would like to know how far Dilly had got with his Enigma studies before Pyry, what he did between Pyry and the outbreak of war, and also what he achieved in the Cottage up to his death in February 1943. It is public knowledge that his organisation, ISK (Intelligence Services Knox), broke an Italian naval cipher system and an Abwehr system both of which used Enigmas different from the German military version. He was probably in touch with Turing's work on naval Enigma. But at the moment I am concerned with matters relating to Huts 6 and 3, and I have found it very hard to determine what Dilly was doing while Hut 6 was getting established. This is no doubt partly due to Bletchley's wartime policy that individuals should know only what they needed to know, but also to Dilly himself. Babbage, who joined Knox around Christmas 1939, has said in a recent letter to me:

> I gradually got to understand the Enigma machine and the problems it posed, but this was mainly through people like Twinn and Kendrick. Dilly was a most entertaining person, but definitely *not* very informative, as you found.

Indeed, it is probable that even Twinn and Kendrick were not fully aware of what Dilly was up to. It is certain that, when I was banished from the Cottage to work in the School, Dilly had told me nothing at all about Pyry, about the perforated sheets that were already being punched, or

about Enigma breaks that had been attempted in the Cottage. Nor was I told about the collaboration with Rejewski's team at Bertrand's Bruno, which seems to have been established in November 1939, when Travis and I were setting in motion the build-up of Hut 6. I am inclined to think, but have no supporting evidence, that this collaboration was handled by Dilly himself, or by ISK if it existed at that time, and that he was, as usual, '*not* very informative'.

In trying to sort out the sequence of events, I have come to believe that Turing took a complete set of the perforated sheets that Jeffreys produced to Bruno on 17 January 1940 and spent a few days with Rejewski and his team. The anecdotes that Rejewski relates about the farewell supper given before Turing returned to England are convincing.[45] For example, Zygalski wondered why each little square in the British version of his perforated sheets had so peculiar a measurement – about eight and a half millimetres on a side. 'That's perfectly obvious', said Turing, laughing. 'It's simply one third of an inch.'

From my memory I would have guessed a later date for the availability of the Jeffreys sheets in Hut 6, but John Herivel's arrival fits in with the 17 January date. He arrived at Bletchley Park on 29 January 1940 and went straight to Hut 6, where Jeffreys and his sheets were already installed. We cannot have been having much success with the sheets at that time, because, once he had got the hang of the machine, Herivel found himself continually wondering how to find a way to break into it. Then, one evening in early February, at his digs, he had the idea of the Herivel tip, or Herivelismus as Kendrick used to call it. He remembers that, when he related his idea to colleagues the following day, it was immediately recognised as a possible way into the Enigma. He thinks that the idea of looking for clusters on a 'Herivel Square' came from me,[46] but I have always thought it was his own. He believes that nothing significant was observed until the German blitzkrieg of May 1940, when suddenly a number of Enigma operators were careless and the 'neighbourhood' of the ring settings for the day stood out clearly on a Herivel Square. This was providential, in view of the fact that the perforated sheets had suddenly become useless.

I myself had nothing to do with the actual breaking of daily keys until the crisis of May 1940, so it is not surprising that, when I was writing my book from memory, I thought that both the Herivel tip and what I mistakenly called 'sillies' were new ideas that occurred to us at that time. Actually the idea of Cillis had been worked on in the Cottage. It is even conceivable that Dilly was aware of them before Pyry. One would like to know. There were a lot of activities in the Cottage of which I was told nothing, as was brought to my attention by Polish accounts of Bruno.

A record was kept at Bruno of all keys broken and exchanged between

B.P. and Bruno from 17 January 1940 to 21 June 1940. What may be deduced from this record is discussed in section VIII. The first Polish break of wartime Enigma came immediately after Turing delivered the Jeffreys sheets, and it seems that Hut 6 started breaking at about the same time. But, in view of Rejewski's impression at Pyry, it is by no means obvious that Dilly and his team did not achieve breaks at a much earlier date. Again one would like to know.

It seems a great shame that the accomplishments of a man who did so much for his country, and indeed for the world, have not been made known. He did outstanding work in Room 40 in the First World War, and stayed on with Alastair Denniston. Around 1936 he was tempted to return to academic life at King's College, Cambridge, but chose to continue his work on Enigma. Not very much is known of his successes with the Enigma machines that were used in the Spanish Civil War. And hardly anything is known of his achievements after that. Of the men who were closely associated with Dilly, both before and after Pyry, the only one alive is Peter Twinn. One would have thought that he would have been encouraged to write about Dilly, but he has been refused permission to do so. One would have thought, also, that the major achievements of other old-timers of GC & CS, such as Oliver Strachey, Josh Cooper, John Tiltman and Hugh Foss, would have been made public by now. Indeed the attitude of the British authorities to the people to whom so much was owed, British as well as Polish, is hard to understand, let alone justify.

Two stories involving Dilly Knox are worth mentioning. Just after the Warsaw–Pyry conferences of 24 and 25 July 1939, Dilly wrote a thank-you note to Rejewski, Zygalski and Rozycki saying, in Polish, 'My sincere thanks for your co-operation and patience'. He enclosed for each of them a set of little paper 'batons', inscribed with the letters of the alphabet.[47] Rejewski's comment was 'I don't know how Knox's method was supposed to work. Most likely he had hoped to vanquish Enigma'. Deavours, who published an article on the method of batons in *Cryptologia* of October 1980, believes that Dilly had actually used batons to break the commercial Enigma during the Spanish Civil War, but has been unable to confirm this.

The other story, as yet unexplained, concerns what was known to the Poles at Bruno and Cadiz as 'The Knox Method'. Lisicki tells me that this involved the Meteo Code, the Herivel tip, and a method of using operator carelessness to determine wheel order. The Meteo Code was a three-letter code used by the Germans for communicating weather information between an airfield and aircraft in flight. It first appeared at the turn of 1939/40, but apparently was not considered worth bothering about until around the time of the invasion of Norway, in April 1940. It was found that a reciprocal permutation was being applied to the letters of each code

group in a message. Then the astonishing discovery was made that this permutation was the stecker permutation of the military Enigma key for the day.

Thus the first step of the 'Knox Method' was to break the Meteo Code for each day, which was not difficult. The next step was to use the Herivel tip, which began to perform well in May 1940, according to Herivel's memory. The third step was to determine the wheel order by an analysis of indicator settings and indicators that was different from the Cilli approach. The rest was easy.

This story of a method that Dilly seems to have made known to the Poles but not to Hut 6 is, I believe, only one of many instances in which Dilly generated ideas and did things without telling people who could have used the information. It would be interesting, for example, to know what Dilly did with the daily keys recovered by the Poles and sent to B.P. from Bruno. These keys could have been valuable in the catalogue of broken keys that was kept in Hut 6 by Reg Parker.[48] Knowledge that the Poles were breaking Green traffic would certainly have been of value to me, but it was not communicated.

It seems, in fact, that even if Peter Twinn is allowed to write an account of Dilly's activities before and during the war, there will be parts of the story that can never be told.

VII

THE BOMBE WAS NOT ALL THAT MATTERED

On page 184 of his official history of *British Intelligence in the Second World War* Hinsley states that the first bombe arrived in August 1940. This I can believe, though from memory I would have guessed September. On page 494 of his Appendix Hinsley changes the time of arrival to the end of May 1940 and goes on to say that 'it is possible to arrive at an actual measure of the Polish contribution to the successes against the wartime Enigma'. His argument leads to the conclusion that, in the absence of Polish assistance, the first bombe would have been delivered in January 1941 instead of in May 1940. This, in my opinion is utter nonsense. Furthermore, as I will attempt to show, the bombe was not all that mattered.

The January 1982 edition of *Cryptologia* contained Rejewski's remarks, dated 2 December 1979, on Hinsley's Appendix 1, a copy of which had been sent to him by Woytak. In comments on 34 of Hinsley's statements, Rejewski shows that the Appendix gives a very inaccurate account of the Polish work. Hinsley is also misleading in his discussion of the British effort. His greatest error, in my view, is his complete failure to grasp the importance of the people who were involved.

It was extremely important that we were able to recruit enough high-

quality people in time to take advantage of the opportunities that came our way. Hinsley was not at Bletchley in the early days and may not have been told of the sheer piracy that we were able to employ in our recruiting until the spring of 1941, when C.P. Snow was put in charge of the allocation of all scientists and mathematicians. Thanks to the Poles we got started quickly and recruited enough key people to see us through the crisis of May 1940. The success of this first round of recruits made it possible to go on recruiting for the expansion of our problems that lay ahead. Without assistance from the Poles, our recruitment of high-quality people would have been too little and too late.

To be more specific, if the Poles had not given us the details of the Enigma at Pyry, the British GC & CS would probably have continued to think that the Enigma problem was hopeless without a capture. Even if Turing had thought of his bombe, there would have been little or no justification for its engineering development. I would probably not have been assigned to work on Enigma, and who else would have thought of the diagonal board? The need for a production-oriented organisation would not have been apparent. If Herivel had not been recruited in January 1940, who would have thought of the Herivel tip, without which we would have been defeated in May 1940 – unable to maintain continuity until the bombes began to arrive many months later?

Let there be no misconceptions about this last point. Loss of continuity would, at all stages, have been very serious, if not disastrous. I feel confident in making this statement, even though I myself knew very little about how the Hut 6 team of 'wizards' dealt with their cryptanalytical problems. I can claim to have made their recruitment possible, early enough and in sufficient numbers. They did the job.

Hinsley was not the only one to concentrate far too much on the bombe. Another, as I have learned only recently, was Oscar Oeser, who was appointed in 1942 to be the spokesman for Hut 3 in matters of priority. In March of 1983 Jean Alington (now Mrs Jean Howard), who had been Oeser's deputy, was asked by the BBC to prepare a statement on the preparations that were made at Bletchley for D-Day. A year later, after talking to a lot of people who had been involved, she submitted a statement[49] and sent me a copy thinking it would be of interest. It certainly was.

What Jean had found most extraordinary about her research was how *little* everyone knew about the whole picture. For instance no one appeared to remember the large log-reading group that had been built up by M18, or the means by which interception had been co-ordinated with Hut 6 activities from the very beginning. She remarked: 'Each individual, working flat out, thought that they knew everything. In fact each individual had tunnel vision.' What happened, I think, is that people who

arrived in Hut 3 after the first two years were put into slots in a well established organisation. Their assigned tasks kept them working flat out and, as Jean says, they did develop tunnel vision.

Jean herself arrived early enough to take part in the formative period in Hut 3. The Air Index, which was to prove of enormous importance, had been set up by Squadron Leader Reggie Cullingham in early 1941. Jean joined him in May 1941, at which time the whole index was contained in one shoebox. Oeser, then a Flight Lieutenant, was already one of the RAF representatives in Hut 3, which was then headed by Commander Saunders. The index, compiled from Hut 6 decodes, soon became a means of indoctrinating new arrivals in Hut 3. Jean remembers indoctrinating Peter Calvocoressi when he arrived early in 1942. Of the authors who have written about Ultra, Calvocoressi, in his *Top Secret Ultra*,[50] seems to me to have the best appreciation of the importance both of interception and of the overall co-ordination achieved by Hut 6 in the early days and maintained throughout the war.

During 1942, just as I was feeling the need for a much closer interrelationship between Hut 6 and Hut 3, the organisation of Hut 3 was changing. Travis asked Saunders to focus his efforts on the obvious need for a greatly expanded bombe programme. Group Captain Jones came in to direct the equally obviously needed expansion of Hut 3. At my request he appointed Oeser, now a Wing Commander, as the spokesman for Hut 3 on matters of priority between our two organisations. When, in 1943, Oeser set up an organisation known as 3L, Jean joined him, leaving the Air Index activity which had grown to six girls on each shift.

I had hoped that Oscar would grasp the whole picture of what really mattered, making it known to key people in both Huts. But it now appears, from what Jean tells me, that this did not happen. He concentrated on bombe time and decoding, for which he developed 'coefficients of importance and urgency'. He himself was often away, leaving the donkey work of the bombe time exercise to Jean and his other assistants. He took little or no interest in the overall picture, and he did little to inform key people in Hut 3 of what was going on elsewhere. This is evidenced by the fact that, at an Anglo/Yugoslav Symposium at the Imperial War College, Jean heard Ralph Bennett, who had been a Hut 3 Duty Officer, state blandly: 'I suppose we just covered frequencies by luck.' She blew her top!

Fortunately the management of interception was in the hands of well qualified people, Commander Ellingworth and Wing Commander Shepherd. When I started to analyse Enigma messages in 1939, I established a close working relationship with Ellingworth at Chatham. At the turn of 1939/40 Hut 6 already had a 24-hour team under Colman, which kept in continual telephone contact with Ellingworth's duty officers.

When, in 1941, the big RAF intercept station at Chicksands was opened, Wing Commander Shepherd co-operated closely with Ellingworth and Colman. Very soon Colman's team was working just as smoothly with the Duty Officers at Chicksands as they were with those of Ellingworth, who had moved his main station to Beaumanor. The organisation that was established in the first two years worked remarkably smoothly for the rest of the war.

The interception and analysis of radio nets carrying messages enciphered on the German military Enigma was not as simple a matter as it has been made out to be. The term 'frequency' as used by Bennett and others is misleading, for the radio sets of those days would drift badly. Each controller of a German radio net would have to struggle to maintain contact with and among his outstations, using chit-chat for this purpose.[51] Each of our intercept operators, struggling to keep in touch with the stations of a radio net, would be continually tuning to pick up the chit-chat. It would have been useless to tell our operators to keep their sets tuned to specified radio frequencies. On the other hand our experienced operators could identify individual German operators by their habits, even when their transmitters had drifted quite badly from assigned frequencies.

The analysis of the radio transmissions started with the intercept operator, who recorded all chit-chat and identifications on sheets of a 'log'. When the German net controller had paved the way for the transmission of an Enigma message, this message would be recorded on a separate sheet. The log sheets would go to the M18 log-reading group, which started in London and moved first to Harpenden, then to Beaumanor, and finally to Bletchley. Except for the time when the group was at Beaumanor, all log sheets reached them by despatch rider. The messages were sent to Hut 6, also by despatch rider, for a good part of the war.

Unfortunately the term 'Traffic Analysis' or TA, when applied to wartime radio nets carrying Enigma traffic, means different things to different people. To some it means obtaining information from a study of the logs. To others it involves enciphered Enigma messages as well as the chit-chat in the logs. When I used the term in my book I meant the analysis of enciphered Enigma messages and their preambles. This, from the outset, was done in Hut 6. The log-reading was done by the M18 group, who ultimately joined forces with Hut 6.

Without going into too much detail I want to show that our method of handling message analysis, well established in the first year and virtually unchanged throughout the war, mattered a great deal. It was based on the 'Traffic Register', which should perhaps have been called the 'Message Register'. It contained the preamble of each message and the first six

letters of enciphered text. This was all that we needed in Hut 6 until we decided how we were going to attempt to break a daily key. The register was sent, page by page, by teleprinter, so there was very little delay between the interception of a message and the time at which its preamble reached Hut 6.

Until May 1940 the register revealed female indicators. Then it enabled us to work immediately on Herivel tips and Cillis. Later on it enabled us to call for important messages to be sent to Hut 6 by teleprinter rather than by despatch rider.

In Hut 6 three copies of the register went to three destinations, to the Registration room, where the messages were charted, to the cryptological wizards, who used them to plan their attempts at breaks, and to Colman's team of intercept co-ordinators, who used them in their constant telephone contacts with duty officers at the intercept stations, who had their own copies of the register pages that they had transmitted. It proved to be a very speedy and efficient system of information exchange between the specialised teams whose contributions were essential to our success. From Jean's research it now seems that leading people in Hut 3 did not realise how this Traffic Register system reduced the delays involved both in breaking and in giving them the most important decodes. It also seems that Oeser and other leaders in Hut 3 contributed little. But there was probably not much that they could do. When the heyday of Ultra had arrived, Milner-Barry's team of wizards, Colman's team of co-ordinators, the large log-reading effort, and the experienced people at the intercept stations could do a good job on their own. It was extremely important that this group of teams were allowed to collaborate without uninformed outside interference.

Indeed the British success in developing and using Hut 6 Ultra was largely due to the early establishment of excellent communication, collaboration and co-operation between many specialised activities. In Chapter 3 of *The Ultra Secret*, Winterbotham recalls how the intelligence part of the overall plan was born. Menzies showed him the 'first results' from Bletchley – four decodes of German air force Enigma messages – and asked him to take them to the Director of Air Intelligence at the Air Ministry. On the following morning Winterbotham presented Menzies with a plan for handling the output of Hut 6. Anticipating problems that would arise later, he proposed that an intelligence organisation be set up at Bletchley to work closely with Hut 6, and also that Special Liaison Units (SLUs) be established to protect the security of Ultra in the field. Menzies said, 'All right, you can go ahead if you can get the approval of the Directors of Intelligence'. The Director of Air Intelligence gave his approval immediately. Then, says Winterbotham, 'As luck would have it,

the next signals to be caught and unbuttoned were from the German Army'.

So he approached the Director of Military Intelligence at the War Office and won his immediate approval. Thus, within a few days; it became possible to establish an inter service intelligence activity at Bletchley and to start building up an organisation of SLUs. That this was achieved so early proved to be of immense importance. However, writing from memory, after more than 30 years, Winterbotham got his dates wrong. He made it seem that all this happened in early April 1940. This error was repeated by Lewin,[52] who also gave the erroneous impression that Hut 6 was not put on a 24-hour footing until just before Hitler's invasion of Denmark and Norway. Hinsley repeats both these errors in his official history. Fortunately a glimpse of the true story is provided by a list of the broken Enigma keys that were exchanged between Bruno and Bletchley during the period of co-operation. It now seems that Hut 6 Ultra was born in mid-January 1940, not in early April.

VIII

LANGER'S LIST OF 126 BROKEN ENIGMA KEYS

Colonel Langer wrote a 48-page report – probably in Algeria in autumn 1940 – on the activities of his Cipher Bureau. This report contains a listing of broken Enigma keys, which is shown in a modified form in Tables 1 and 2. Table 1 starts with the last daily key broken in Poland before the war – a key for 6 July 1939, broken on 26 August, 1939. The other entries in Table 1 are daily keys of 1939 broken at Bruno or Bletchley in 1940.

Table 2 is concerned with daily keys of 1940. In this table it has been convenient to show the delay in days between the date of a daily key and its entry in Langer's list of broken keys. Polish breaks would have been recorded at once, but Bletchley breaks could not be entered until they had been communicated to Bruno, which evidently took many days in the early months of collaboration.

Unfortunately Langer's list does not indicate which of the German crypto nets (Red, Green or Blue) was involved in each break. Nor does it say which of the breaks were achieved at Bruno. But we have clues, and it is intriguing to speculate on what may have happened.

In his rebuttal of much of the content of Hinsley's Appendix 1 to Volume 1,[53] Rejewski agrees that 83 per cent of the keys in Langer's list were broken at Bletchley. This means a score of 105 for Bletchley and 21 for Bruno. He also points out that at Bruno everything had to be done by Zygalski, Rozycki and himself, whereas Bletchley already had far more people at work. Indeed the Polish achievement of 21 breaks is quite

remarkable, remembering that this same team of three would be deciphering messages on daily keys broken at Bletchley.

It seems clear that the first break at Bruno was the daily key for 28 October 1939, broken on 17 January 1940, immediately after the arrival of perforated sheets from Bletchley. This was the Green key used by the administrative centres of the German army. It also seems clear, though surprising to me, that the Green key for 25 October 1939 was broken at Bletchley at about the same time.[54] Apart from this one key I suggest that the remaining nine daily keys of Table 1 were Polish breaks.

TABLE 1
DAILY KEYS OF 1939
(shown on Langer's List of Breaks)

Date of Daily Key (in 1939)	*Date of Break*
July 6	August 26 1939
August 2	January ? 1940
September 3	January 28
September 10	March 17
September 13	March 17
September 19	February 28
September 29	February 23
September 30	February 13
October 25	January 27
October 28	January 17

In the period covered by Table 2, there are 16 cases in which two different daily keys for the same day were broken. I suggest that the Poles broke the first of the keys shown in the table for the following seven days: 6, 16, 18, 26 January, 24, 27 February and 20 March; also that they broke the second keys on five days: 18 January, 21 February and 2, 21, 27 March. This accounts for the Bruno score of 21 breaks. Those shown on Table 2 are italicised. Much of this is pure conjecture, but it may well be pretty accurate.

It appears that, after the sheets were received on 17 January 1940, the Polish three-man team worked backwards, leaving work on current keys to Bletchley. I suspect that they concentrated on Green traffic, while we concentrated on Red. As I discovered in my studies of September and October 1939, the French intercept stations were far better placed for the interception of Green traffic than was our station at Chatham under Commander Ellingworth.[55] Furthermore, I found that the call signs were repeated monthly, so the French traffic analysts, as a result of observation over a long period, would have been able to provide a complete forecast of call signs for each day. This would have been a great help to

TABLE 2

DELAYS IN DAYS BETWEEN THE DATE OF A DAILY KEY OF 1940 AND ITS ENTRY ON LANGER'S LIST OF BROKEN KEYS

Date of Daily Key	*Delays Jan.* A	B	*Delays Feb.* A	B	*Delays March* A	B	*Delays April* A	B	*Delays May* A	B	*Delays June* A	B
1					14				1		0	
2					6	*24*			0			
3							1		1			
4					7	14			2		0	
5									7		0	
6	*19*				5				1		0	
7					4				2		0	
8			15		4		1		1		0	
9					2		3	6	1			
10							4	4	1			
11							1		1		0	
12			15		4	5	4		1		0	
13			14		4	8			1		0	
14			9				2		1		1	
15							1				6	
16	*43*		10		2		1				5	
17	11						1					
18	*34*	*41*					2					
19							1	5				
20			6		*17*		1		1			
21			7	*23*	2	*19*	1	1	0			
22	12		4		8	11	1	1	1			
23			8		3		1	2	1			
24	15		*23*				1		1			
25					8		1	1	0			
26	*28*						1		1			
27			*31*		2	*13*	0		*0*			
28							2		1			
29	10		4				1		0			
30	14		X		9		1		1			
31	5		X				X		0			

Columns A and B allow for cases in which two different daily keys for the same day were broken.

intercept operators because, as Ellingworth explained to me, the German radio net carrying Green traffic used an unusual method of operation which made it difficult to intercept.[56] Anyway, using available Green intercepts, the Poles attacked the Green key for 6 January 1940, which they broke on 19 January, only two days after the arrival of the perforated sheets. Next, on 28 January, having no doubt spent a lot of time decoding messages on the two broken keys, they broke the Green key for 3 September 1939. In February and March of 1940 they went back to Green traffic of 30, 29, 19, 13, and 10 September 1939. This is shown in Table 1.

They also managed to attack current traffic of several days in January, February and March of 1940, as shown in Table 2: a truly remarkable achievement by Rejewski, Zygalski and Rozcyki.

Because I have no recollection whatever of an early break of Green in Hut 6, I think that the Bletchley break of the Green key for 25 October 1939 must have been made in the Cottage around 17 January when a complete set of perforated sheets had become available. The Hut 6 activities were based on intercepts received from Chatham, and I am pretty certain that these would not have permitted a break of Green at that time. On the other hand French intercepts may well have been made available to Dilly's team in the Cottage.[57]

Let us suppose that, after completion of the Jeffreys sheets, the first two Bletchley breaks, both made in the Cottage, were the Red key of 17 January 1940,[58] and the Green key of 25 October 1939. This would tie in with Winterbotham's account of the Enigma decodes that Menzies showed him.

As yet, I have not been able to determine just when Jeffreys, with his team and their sheets, moved from the Cottage to Hut 6. It was certainly before 29 January 1940, when John Herivel arrived at Bletchley and found Hut 6 operational on a 24-hour footing. He remembers that early in February, when he had got the hang of the machine, he was concerned by our lack of success (the table shows no breaks between 31 December and 8 February) and found himself continually thinking about what could be done about it. Then, one evening in his digs, when he was imagining what it would be like to be a German operator preparing to send off his first message of the day, the idea of his 'tip' flashed into his mind. His recollection, however, is that the tip did not become significant until the German Blitzkrieg of 10 May 1940, when suddenly a number of German operators simultaneously showed the appropriate form of laziness.

Looking at Table 2, it seems possible that the move to Hut 6 occurred between 17 and 22 January, and that the broken keys of 22, 24, 29, 30 and 31 January were Red. But I am still puzzled by my memory that the first Hut 6 break was into the Blue crypto net used for training.[59] Perhaps the key for 22 January was of Blue and the double breaks of March were of Red and Blue.[60] I feel sure that the 24-hour operation of the supporting activities in Hut 6 had started before Jeffreys arrived, in fact in early January 1940, or in late December 1939.[61] This was one of the things that really mattered.

We now come to the spectacular changes in Langer's listing that occurred in April, May and June of 1940. Going by the delays in Langer's recordings of Bletchley breaks, it seems that direct teletype communications between Bletchley and Bruno were not established until late March or early April. More important is the fact that regular breaking of Red

traffic began on 8 April, when the Phoney War ended with preparations for the invasion of Denmark and Norway on the following day.[62]

The gap in breaking between 14 and 20 May was, of course, caused by the German change of procedure, which made our perforated sheets useless.[63] Note that the date on which the change became effective was 15 May, which fits in with my memory, not the commonly accepted 10 May, the day on which Hitler's invasion was launched. Indeed, as was shown in section V.1 above, the Germans seem to have developed a habit of making major changes on the fifteenth day of a month.

The resumption of Hut 6 breaking on 20 May, after a lapse of only five days, was not due, as Hinsley claims on page 494 of his Volume 1, to the arrival of the first bombes. It was due to German operators who, working no doubt under unprecedented pressure, suddenly made the Herivel tip effective and provided enough Cillis to exploit it. Note the increasing number of zeros in Langer's list. This was due to the fact that the Herivel tip depended on the first messages sent by lazy operators after a midnight key change. With the old method we had to wait until enough female indicators had appeared before we could start stacking perforated sheets. Now, if German operators provided enough Cillis as well as a good Herivel tip, the break of a daily Red key could sometimes be achieved in Hut 6 by the midnight to 8 a.m. watch. Again, as with the old method, the Traffic Register from Chatham provided our Machine Room with all the necessary information.

It may seem barely credible, but comparable success, using the Herivel–Cillis method, was maintained until the actual arrival of the bombes. On page 184 of his Volume 1, Hinsley contradicts his other statement, saying that the first bombe was delivered in August 1940, but I suspect that it may have been even later. My guess would be that the bombes did not begin to be effective until September 1940. We were indeed lucky.

REFERENCES

References are given in chronological order of publication. Not all are mentioned in the article.

1. David Kahn, *The Codebreakers: The Story of Secret Writing* (London: Weidenfeld & Nicolson, 1967).
2. J.C. Masterson, *The Double-Cross System in the War of 1939–45* (New Haven: Yale University Press, 1972).
3. David Kahn, *The Codebreakers* (abridged) (London: Sphere, 1973).
4. Gustave Bertrand, *Enigma, The Greatest Riddle of World War II* (Paris: Plon, 1973).
5. F.W. Winterbotham, *The Ultra Secret* (London: Weidenfeld & Nicolson, 1974).
6. Anthony Cave Brown, *Bodyguard of Lies* (London: W.H. Allen, 1975).
7. William Stevenson, *A Man Called Intrepid: The Secret War* (London: Macmillan, 1976).

8. Penelope Fitzgerald, *The Knox Brothers* (London: Macmillan, 1977).
9. Ronald Lewin, *Ultra Goes to War: The Secret Story* (London: Hutchinson, 1978).
10. David Kahn, *Hitler's Spies: German Military Intelligence in World War II* (London: Hodder & Stoughton, 1978).
11. Brian Johnson, *The Secret War* (London: BBC Publications, 1978).
12. R. V. Jones, *Most Secret War* (London: Hamish Hamilton, 1978).
13. Wladyslaw Kozaczuk, *W Kregu Enigmy* (Warsaw: Ksiazka i Wiedza, 1979).
14. F. H. Hinsley, *British Intelligence in the Second World War* (London: HMSO, Volume 1, 1979; Volume 2, 1981).
15. 'The Polish, French and British Contributions to the Breaking of the Enigma' (Appendix 1 to Vol. 1 of ref. 14 above, 1979).
16. Ralph Bennett, *Ultra in the West* (New York: Scribner, 1979).
17. Jozef Garlinski, *The Enigma War* (published as *Intercept*, London: Dent & Sons, 1979); (New York: Scribner, 1980).
18. Peter Calvocoressi, *Top Secret Ultra* (London: Cassell, 1980).
19. Jean Stengers, 'La Guerre des Messages Codés (1930–1945)', in *L'Histoire*, February 1981.
20. Marian Rejewski, 'How Polish Mathematicians Deciphered the Enigma' (published posthumously in Polish in Poland, 1980), translation published in *Annals of the History of Computing*, July 1981. (Another translation published as Appendix D in ref. 30, 1984.)
21. Marian Rejewski, 'Mathematical Solution of the Enigma Cipher' (published posthumously in Polish in ref. 13, 1979), translation published in *Cryptologia*, January 1982, and copied as Appendix E in ref. 30, 1984.
22. Christopher Kasparek and Richard A. Woytak, 'In Memoriam Marian Rejewski', *Cryptologia*, January 1982. (Part of it appears as Appendix A in ref. 30, 1984.)
23. Wladyslaw Kozaczuk, 'Enigma Solved' (excerpts from ref. 30) in *Cryptologia*, January 1982.
24. Richard A. Woytak, 'A Conversation with Marian Rejewski' in *Cryptologia*, January 1982 (recorded on tape in Polish, 24 July 1978, and reproduced as Appendix B in ref. 30, 1984).
25. Marian Rejewski, 'Remarks on Appendix 1 to *British Intelligence in the Second World War* by F.H. Hinsley' (letter to Woytak) in *Cryptologia*, January 1982.
26. Gordon Welchman, *The Hut Six Story: Breaking the Enigma Codes* (London: Allen Lane; New York: McGraw Hill, 1982).
27. Ronald Lewin, *American Magic* (New York: Farrar, Straus & Giraux, 1982).
28. Andrew Hodges, *Alan Turing – The Enigma* (London: Burnett Books, 1983).
29. Jean Stengers, 'Enigma, the French, the Poles and the British, 1931–1940' in C. Andrew and D. Dilks (eds.), *The Missing Dimension* (London: Macmillan, 1984).
30. Wladyslaw Kozaczuk, *Enigma – How the German Machine Cipher was Broken and How it was Read by the Allies in World War Two, with Appendices A to F* (edited and translated by Christopher Kasparek, London: Arms and Armour Press, 1984).

NOTES

1. See ref. 4.
2. See ref. 5.
3. See ref. 26.
4. See ref. 19.
5. See ref. 17. It was called *Intercept* in the UK, where it was published in 1979.
6. See ref. 21.
7. See ref. 20.
8. See ref. 29.
9. See ref. 30.
10. See ref. 13.
11. See ref. 15.

12. See ref. 28.
13. See Chapter 5, *The Hut Six Story*.
14. *The Hut Six Story*, pp. 170–76.
15. When I was writing *The Hut Six Story* I knew nothing of the work in the Cottage on Cillis. I called them sillies, and my account of how they worked is quite wrong. This was pointed out to me by Dennis Babbage, who was an expert. The correct account is far more fascinating. After reading my book, Lisicki told me of a somewhat similar method known to the Poles as 'the Knox Method'.
16. See ref. 9.
17. See ref. 27.
18. Kozaczuk, *Enigma*, p. 235.
19. *The Hut Six Story*, p. 16.
20. Ibid., p. 13.
21. In my discussion of the Bletchley Park environment I mentioned that the expression 'cock and bull story' is said to have originated in Stony Stratford, where there are two famous pubs, the Cock and the Bull. *The Hut Six Story*, p. 187.
22. In Kozaczuk, *Enigma*, pp. 249 and 276 respectively.
23. Ibid., p. 249.
24. These drums are described in *The Hut Six Story*, pp. 307 and 308. Similar drums appear in the picture of the American version of the bombe in Lewin, *The American Magic*, facing p. 142.
25. See *The Hut Six Story*, pp. 38ff.
26. Their method of operation is discussed in *The Hut Six Story*, pp. 153–6.
27. Some writers have used the word 'setting' to mean the daily key.
28. *The Hut Six Story*, p. 169.
29. Kozaczuk, *Enigma*, p. 265.
30. Ibid., p. 246.
31. *The Hut Six Story*, p. 46.
32. Ibid., p. 50.
33. See Kozaczuk, *Enigma*, p. 258.
34. Ibid., pp. 284 and 285.
35. Ibid., p. 264.
36. Ibid., p. 266.
37. The construction of the bomba is indicated by Rejewski in Figure E–8, Kozaczuk, *Enigma*, p. 289.
38. His train of thought is indicated in Kozaczuk, *Enigma*, p. 287.
39. The principle is more fully explained in *The Hut Six Story*, Chapter 4. A Zygalski sheet is illustrated in Figure E–7 in Kozaczuk, *Enigma*, p. 288.
40. They had been issued in 1936 with the idea that they would be brought into use when war became imminent. Kozaczuk, *Enigma*, p. 64.
41. Calvocoressi (see ref. 18) was incorrect in saying that, at this time, no one in the world could read messages enciphered on the five-wheel Enigma.
42. Kozaczuk, *Enigma*, p. 236.
43. Ibid., p. 257.
44. *The Hut Six Story*, p. 307.
45. Kozaczuk, *Enigma*, p. 97.
46. *The Hut Six Story*, p. 100.
47. Kozaczuk, *Enigma*, p. 60.
48. *The Hut Six Story*, p. 131.
49. This statement was not used in the BBC programme for the anniversary of D-Day. This was perhaps just as well, because Jean had been given a lot of misinformation.
50. See ref. 18.
51. See *The Hut Six Story*, Chapter 9. The chit-chat used the international Q-Codes, still widely used today (p. 154).
52. See Lewin, *Ultra Goes To War*, p. 60.
53. See *Cryptologia*, Vol. VI, No. 1 (January 1982), pp. 74–83.
54. The date of this Bletchley break is stated to be 18 January 1940, on p. 662 of Hinsley's

Volume 2. However, his earlier account in Vol. 1, p. 493, is, I believe, inaccurate.
55. *The Hut Six Story*, p. 54.
56. The monthly repeat of call signs was discontinued soon after I discovered it.
57. I was given large bundles of these intercepts in September 1939. See *The Hut Six Story*, p. 54.
58. I think that Hinsley was misinformed in stating that the Red key for 6 January 1940 was broken at Bletchley on the same day.
59. *The Hut Six Story*, p. 88.
60. Hinsley, vol. 2, p. 659, gives 29 January as the date on which Blue was first broken, but he gives 6 January for Red which seem wrong.
61. *The Hut Six Story*, p. 89.
62. The second breaks into keys for 9, 10, 19, 21, 22, 23 and 25 may have been into the Yellow key, which, according to Hinsley (Vol. 2, p. 662) was first broken on 10 April. I have no recollection of the introduction by the German army of a second crypto net for operations in Norway. The key that we broke regularly from 8 April on was certainly the Red key, used in battle for army–air co-ordination. To me the Yellow crypto net is still a puzzle.
63. *The Hut Six Story*, p. 97.