COLOSSUS

BLETCHLEY PARK'S GREATEST SECRET

'Masterly.' *Spectator*

PAUL GANNON

Appendix A - Fish Chronology

1940

May	First non-Morse transmissions heard, but not followed up due to lack of resources and concentration on Enigma Swedish codebreaker, Arno Beurling, breaks the Siemens T52 version of the Geheimschreiber used on landline between Denmark and Norway.

1941

April	Research Section set up under Colonel John Tiltman and Major Gerry Morgan More non-Morse Baudot/teleprinter and Hellschreiber transmissions detected and experiments with new directional wireless techniques.
May	Bill Tutte and Jack Good join GC&CS
June	First 'Tunny' (Lorenz SZ40) link opens between Vienna and Athens. Work in Research Section starts on wireless teleprinter cipher. Hitler launches invasion of Russia, 'Barbarossa'.
August	The depth 'HQIBPEXEZMUG' is intercepted & read.
September – December	Whole of Research Section works on trying to analyze the key produced by the depth
November	Norwegian secret agent passes information about Swedish break of the Siemens T52 to GC&CS
December	GC&CS considers exchanging information on the SZ40 with the Russians in the hope that they may provide useful information in return. Russia counter-attacks at Moscow; Japanese attack on US fleet at Pearl Harbour; Germany declares war on USA.

1942

January	'Tunny' Machine broken for August 1941 following Bill Tutte's analysis of the key produced by reading the depth. References to 'Geheimschreiber' intercepted on non-Morse links during operator 'chat'.

March	GC&CS identifies four 'Non-Morse' groups in operation (NoMo1 – 4) Broken traffic shows pin patterns re-arranged, so preventing Tutte's technique for analyzing the key from a depth Tone transmission replaces Hellschreiber
April	First 'Tunny analogue' machines ordered GC&CS breaks the SZ40 Geheimschreiber for March 1942 First attempts at Chi setting References to 'Saegefisch' intercepted in chat on non-Morse lines and on parallel Enigma/Morse wireless links. Decision taken to set up special non-Morse wireless interception station
May	Wheels broken before the end of the month by the indicator method
June	First 'Tunny' analogue arrives Land requisitioned for 'Knockholt' non-Morse wireless interception station on the North Downs in Kent.
July	Testery founded to take over work from Research Section Current traffic read for the first time Turingery method introduced Montgomery reverses defeats in desert, halting Rommel at Alam Halfa
August	Introduction of 'Quatsch' (nonsense text) Interceptions begin at Knockholt.
October	Experimental Tunny link closed, replaced by link called 'Octopus'. 'Codfish' link to South Russia opens. Use starts of QEP systems and monthly change of Psi patterns Testery confined to depths Research Section starts to investigate statistical methods Battle of El Alamein. Max Newman joins GC&CS
November	New 'Fish' links to Russia intercepted Newman suggests electronic counters 1+2 break in invented by Tutte for implementing statistical approach Message set statistically using delta-cipher-1 + delta-cipher-2 rectangle
December	Newman given task of developing machines for setting Tunny German 6 Army surrounded at Stalingrad. Herring link opens between Rome and North Africa

1943

January	Early Robinson designed and ordered. Knockholt goes into full production.
February	DZ4JA (with Chi-2 limitation) makes first appearance on Codfish Research Section breaks Chis statistically from cipher text by rectangles
March	X2 P5 limitation tried experimentally on Herring Plans for mechanical setting of Tunny and Sturgeon well under way X2 limitation broken
April	First sixteen Wrens arrive X2 P5 broken by Testery and Research Section Fish decrypt reveals German plans for attack on the Kursk salient, operation 'Zitadelle'.
May	Method of contracted de-Chi successful Axis forces in North Africa surrender and two Geheimschreibers captured. Beginning of month Bream link, between Rome and Berlin, opens. The link is broken by the end of the month. It was to be the most productive of all Fish links in terms of value and volume of intelligence.
June	Newmanry starts work Arrival of Heath Robinson First Newmanry 'Tunny analogue' (a more complex machine than the first 'Tunny' analogues Allied invasion of Sicily.
July	Battle of Kursk. German offensive, 'Zitadelle' fails and Russian army launches major counter-offensive. Fall of Mussolini.
August	Discovery that Knocholt was producing a lot of 'slides' in tapes
September	Suggestion of 'and/or' machine and repeated use of character in Colossus and Robinson Discovery that best delta-P letter is not necessarily / Expected score of motor run in terms of delta-D Allied landings in southern Italy.
October	Changeover from two to three shifts German military occupation of Italy.
November	Newmanry moved from Hut 11 to Block F First production Robinson arrives

Recognition that de-Chis can be broken by hand

December
Reappearance of X2 + P5 limitation in Bream and Codfish traffic
Testery take on Psi and motor setting and Newmanry concentrate on Chi setting and breaking
Second production Robinson arrives
Recognition that delta-D statistics (rather than delta-P) are the quickest way of finding new keys.

1944

January
General Registeries of the Newmanry and Testery amalgamated
Direct teleprinter line from Knockholt to Block F installed
Robinson 3 (first double bedstead machine) installed
X5 now set in Newmanry rather than sending de-Chis on only four impulses [units] to Testery
Jellyfish link, Paris to Berlin, opens

February
Colossus I installed
Spanning suggested
Colossus first used for wheel breaking

March
Robinson IV installed
Jellyfish first broken (using a 'crib' from Bream)

April
First motor runs successfully done on Colossus
New Tunny analogue machine, new Garbos and one Mrs Miles installed
Significance tests for rectangles

May
Cribs predicted by Sixta successfully used for wheel breaking for the first time

June
D-Day – Allied invasion of North-West Europe
SZ40B first used on Codfish with X2 Ps1 P5 limitation
Daily meetings started
Colossus II installed
First indications of change of wheel pin patterns becoming more frequent than once a month.

July
Daily wheel changes on Jellyfish
Koenigsberg exchange closes and moves to Zossen
Slide runs started using test tapes to check machines

	Colossus III installed More reliable Robinsons designed, suitable for work on cribs New 'staircasing' method evolved for cribs Significance tests for wheel breaking runs introduced
August	Daily wheel changes on almost all Tunny links Number of computers [i.e. human operators] increased very considerably First rectangles made on Colossus Colossus IV installed.
September	Several links cease using the P5 limitation Work starts on Block H Colossus V installed Thurlow rectangles first done Combined X3 flag for key introduced with significance test
October	Further reorganization of Tunny Colossus VI and first super-Robinson installed Colossus VI takes tapes up to 25,000 characters long Copy correction checks (for correction of tapes) introduced
November	15th November The Fire New type of test runs for checking Colossus test runs Kedlestone Hall starts operating Knockholt reorganized Colossus VII installed New adaptations of rectangling methods used to break short stretches of key
December	P5 limitation largely abandoned by the Germans Extensive motor and Psi setting by machine Colossus decoding invented Theory of coalescence
1945	
January	Psi test runs first made De-Chi checks first done Education committee first formed Colossus VIII installed Second super-Robinson finished
February	Device installed on Colossus VI enabling rectangles to be computed quickly Rectangles now produced on tape to mechanize computing on keys

	Colossus IX installed Tests carried out on Thrasher (on new Robinsons) give negative results with regard to Tunny type machines
March	Exchange set up at Salzburg Mechanical flags instituted Wrens taught wheel-breaking Machine tested regularly by Wrens
April	Rectangle making started on super-Robinsons Colossus X installed US 5020 ‘optical’ machine arrived to start work experimentally
May	Victory in Europe Last Tunny message sent Change from three to two shifts Work on back traffic (1942-4) History and 5202 Sections formed
June	Two sets of German Tunny equipment arrive Experimental operations using 5202 Experimental work on Colossi for non-Fish purposes

Appendix G - Communications and the Stalingrad 'Kessel'

The most famous battle of the war on the eastern front was at Stalingrad in 1942 and 1943, and it was during those momentous months of attack and counter-attack that the non-morse communications system first came into use by German army units in the Soviet Union. At the core of Hitler's strategy for 1942 were deep thrusts into the south of the Soviet Union, towards the Caucasus, where he sought oil, and towards the Volga and beyond. His response to the challenge of space was to raise the stakes and gamble on as much space again. On the Volga lay the city of Stalingrad. It was not an important military target, just one more city to be taken under control and handed on to the extermination squads which followed immediately behind the German army. The objectives were the forward march to acquire territory and to annihilate the Soviet army, which was again assessed to be on the point of collapse. The German army was expected to move forward very quickly and the headquarters of the German army groups involved in the assault might well need to move locations. It was in this second phase of the assault on the Soviet Union, one of history's blackest episodes, that the new radio and teleprinter system was widely used. Telephone and telegraph wires and poles were erected for the advance, but the ebb and flow of the fronts made radio communications a necessity.

The headquarters of the Army Group South was to over 1500 kilometres from the headquarters of army command near Koenigsberg. The second non-Morse system to be detected by British interception units, providing radio communications on part of the link between the Baltic and Black seas, came into service in November 1942 to provide communications to Army Group South in its drive into the Soviet Union's expectedly soft underbelly. Over the next year half-a-dozen other non-morse links came into use on the eastern front linking army and army group headquarters.

Although the German advance covered spectacular distances in the drive towards the Caucasus, the neighbouring advance to the Volga became bogged down in fierce resistance around Stalingrad and the epic battle for that battered city fired the passions of both sides. The German assault was led by the 6th Army, part of 'Army Group B'. The headquarters of the army group, some distance to the west, and of the 6th Army were connected by 'field cable' buried in the ground, allowing voice and teleprinter communications to and from the forces besieging Stalingrad. The city's capture or successful holding out would take on a significance that was out of all proportion to its military importance. Stalingrad may not have been the most decisive military battle of the war, but it was undoubtedly the most important in terms of propaganda. German intelligence failed to appreciate the forces the enemy could muster, estimating again that the Soviet army had run out of soldiers and weapons. Hitler all but announced the capture of Stalingrad. Yet, as happened the year before at Moscow, the Soviet army had gathered substantial reserves for another unexpected counterblow - one which signified Soviet potential to reverse the roles of the two colossal war machines. The German 6th Army under Paulus was treated to a Soviet display of how to carry out a pincer movement. In German such an encirclement is a 'kessel', usually translated as 'kettle' or 'cauldron',

though the term also refers to a basin-shaped valley and as well to a semi-circular ring of hunters slowly enclosing their prey. In military usage the circle is completed and there is no escape.

In one way the siege of the 6th Army presaged some aspects of modern warfare, where we have become used to television and radio reporters broadcasting, often live, from within war zones – Beirut, Sarajevo, Baghdad spring to mind – rousing public sympathy for the plight of those on the receiving end. For while quite a few of Paulus's soldiers (and their Soviet prisoners) starved to death, and the German army's supply of armaments dried up preventing effective defence against the surrounding Soviet troops, those caught up in the kessel did at least have ample communications facilities. Paulus commented that without the signals corps it wouldn't have been possible to "hold the kessel". In that case, in one sense at least, he may have been better off without such modern communications - Hitler's order to stay put might not have been received and the encirclement avoided. But Paulus did receive the order and obey it he did, organizing his forces in the expectation of rescue. And if he had disobeyed the Fuehrer's instructions, the chances are that the siege would have happened anyway. "In an age when every headquarters was in constant touch by radio, courier and teleprinter, the order for the commander's arrest would be communicated immediately."[1]

The German troops couped up in the kessel also had their own interception and cryptanalytic unit which successfully broke the field ciphers of the surrounding Soviet armies up till mid-December 1942; the intercepted messages giving forewarning of Soviet attacks.[2] However, neither codebreaking nor modern communications technology did the 6th Army much good. There had to be daytime radio silence within the kessel – any transmitter would immediately attract the attention of Soviet intercept teams with direction finding equipment, leading in turn to artillery attack. Instead the 6th Army used its own communications network of cables. The 'field cable' system ran from each of the main command posts to other posts with a mesh of connections ensuring that every unit had at least three independent communications channels (see diagram 6.2). For the first three days there was even a cable link that went outside the kessel. After theSoviet troops discovered the cable communications to German forces to the outside world were based on radio communications during the night.

For the first few weeks of the siege aircraft could enter and leave the kessel bringing in supplies and taking out the wounded. Fellgiebel, ordered a short wave transmitter system – known by the code name 'Saegefisch' – to be flown in allowing radio telephone and radio teleprinter transmission. An antenna was erected each night under cover of darkness and taken down before dawn. Soldiers, when they learnt of the link, queued up to use the radio telephone to call back to Germany. One soldier was even married to his sweetheart at home via the radio link. Its main purpose was to help the defence of the kessel however. In that the link brought first good news – a planned rescue bid by the battle-hardened Field Marshall von Manstein. Then it brought bad news – the failure of Manstein's attempts to break through the surrounding forces.

On the 23rd December 1942, Paulus, caught up in the kessel, and Manstein, well outside it, discussed the situation by teleprinter 'conference' over the radio link. "Paulus asked whether he had finally received permission for the 6th Army to break out. Manstein replied that he still had not obtained agreement from supreme headquarters. He was sparing with the details. If Paulus had been given sufficient information to update his operations map, he would have seen that the 6th Army was beyond help."[3]

1 ABeevor,Stalingrad:theFatefulSiege1942-1943,London1998,276
2 WArnold,BerichtanFellgiebelueberdenEinsatzderNachrichtentruppeinStalingrad,inKWildhagen
3 ABeevor,Stalingrad,302