Der Fall WICHER: German Knowledge of Polish Success on ENIGMA

BY JOSEPH A. MEYER

~~*Top Secret Umbra*~~

In 1939 the Germans found evidence, including decrypts, that a Polish cryptanalytic organization, WICHER, had been reading the ENIGMA. Documents and interrogations did not reveal how the machine could have been read, and after some changes in the indicator system and pluggings, the matter was dropped. In 1943, further evidence of prewar Polish success, and the strong appearance that Navy ENIGMA was being read by the British and U.S., caused a crypto-security crisis. A spy in the U.S. Navy Department reported the reading of U-boat keys. ENIGMA security was studied, and many changes in the machine and its usage were undertaken. By 1944 the Germans acted and spoke as if they knew ENIGMA traffic was being read by the Allies, but they suspected betrayal or compromise of keys. Medium grade ciphers were also improved, and radio security was much improved. Users were forbidden to send secret or top secret information or operational orders over ENIGMA. Through all of this, German confidence in the TUNNY cipher teleprinter (which was also being read) never wavered. The key to German suspicions of ENIGMA appears to have been the knowledge of Polish prewar successes, after which the wartime ENIGMA exploitation hung by a thread for five and one-half years.

I. DER FALL WICHER*

In late 1939, after their rapid conquest of Poland, the German OKH (Oberkommando des Heeres, Army High Command) and OKW (Oberkommando der Wehrmacht, Armed Forces High Command) cryptanalysts obtained definite proof, including decrypts of German messages, that the Poles had been reading ENIGMA messages for several years before the war.[1] Alarmed, the Germans did further security studies on the machine and changed the indicator system in 1940. They tried to track down the French connection after the fall of France in the same year. Later in the war they received further disclosures of Polish success from two prisoner-of-war Polish officers from the

*"The WICHER Case," *Naval Sigint VII*, p. 157, gives an account which appears to differ from this in some details (see reference 11).

Warsaw Cryptanalytic Bureau,[2] and they even learned the name of the project, viz., WICHER (or possibly WICHURA, which means "storm" in Polish); however, their confidence in the security of the machine was never undermined.[3]

The key factor in causing the German cryptanalysts to disbelieve that the ENIGMA was readable and had been exploited was apparently the tight compartmentation of the work in Poland, and later in France.[4] This was further helped by the way the Germans handled the information. The Poles who disclosed the ENIGMA success were Army officers too high up in the Warsaw Cryptanalytic Bureau to explain the details of the work, i.e., *how* it was done, and the young cryptanalysts who did know were either not captured or not interrogated.[5] As a result, the German cryptographers were never forced to an understanding of how the machine could be solved. They were told, but not shown.

In 1938 German invasions of Austria and Czechoslovakia gave them access to the cryptanalytic bureaus in these countries, and they received some surprises, but nothing that weakened their confidence in ENIGMA (see below).

When German forces swept into Poland on 1 September 1939, their Panzer units reached the outskirts of Warsaw by 8 September, but Polish forces continued counterattacks until 19 September and Warsaw itself held out until 27 September.[6] The Polish Government fled to Rumania on 18 September.[7] But the delay in capturing Warsaw, and the Russian attacks, which began on 17 September, gave the Warsaw cryptanalytic bureau a clear forecast of the outcome and sufficient time to destroy records and evacuate key personnel and equipment. There were four young Polish mathematicians who had solved ENIGMA, and they and documents and equipment were evacuated to England and France.[8]

Earlier, when Czechoslovakia fell in 1938, some German cryptanalysts from OKW went to Prague and visited the Czech cryptanalytic organization, which was headed by an officer named Ruźek.[9] The senior OKW member of this party, W. Fenner (later head of OKW/Chi Oberkommando der Wehrmacht/Chiffrierdienst, Armed Forces High Command/Cipher Service), was instructed not to carry out a detailed interrogation. The Czechs disclosed their work and were offered jobs in OKW/Chi, which they refused.[10] They had read German military double transposition after getting pinched information,[11] and subsequently had destroyed all their papers.[12]

There was some confusion among the various German SIGINT parties about whether the Czechs had read ENIGMA or not. Mettig of OKH claimed in 1945 that the Czechs had read traffic from the unsteckered ENIGMA before the war.[12A] Wendland of OKH, in an interrogation on 26 September 1946, also claimed that the Czechs had

read the ENIGMA in "the old system."[12B] But Fenner of OKW, who made the trip to Prague in 1938 and interrogated Ružek, was crossexamined on 30 September 1946 by the same ASA people who had just spoken to Wendland, and Fenner stated clearly that the Czechs never claimed to have read the ENIGMA; this was supposed to have been done by the Polish WICHER organization which was captured in Czechoslovakia.[12C]

Another OKH SIGINT member, Barthel, claimed that before the March 1938 Anschluss the Austrian Cryptanalytic Service had succeeded in "reconstructing analytically" the settings of the ENIGMA and on occasion they could find the daily key and read some German traffic—but this does not seem to have alarmed the Germans.[12D]

When Poland fell, a group of Polish cryptanalysts, apparently known as the WICHER organization,[14] was captured in Czechoslovakia.[13] Ružek apparently informed the Germans, for his name is mentioned in the Fall WICHER context by Hüttenhain of OKW.[15] Two cryptanalysts from OKW, viz., Fricke and Pietsch, were sent to interrogate them.[16] The Poles maintained that they had broken the German ENIGMA but no concrete results came from the interrogation, and no details of the method were obtained.[17] The documents the Poles had were sent to Hauptmann Kempe of OKH.[18] Because of bad feeling between Fenner of OKW and Kempe of OKH, Kempe held onto the documents and told Fenner only "that from these documents it was clear the ENIGMA had been broken".[19] Fenner was never able to see the documents himself, and even after the war was unwilling "to state it as a fact that the Poles in fact achieved this success".[20] (Fenner had been involved in the stecker-pair plugging modification with Dipl. Ing. Willi Korn of Heimsoeth & Rinke in the technical development of the machine in the 1926-32 period.)[21] Fenner thought it likely that the Poles might occasionally, under favorable circumstances, have read a depth, but discounted reading of messages or whole series of messages.[22]

Mettig in 1945 claimed that three deciphered messages from a German cruiser in Spanish waters during the civil war in 1937 were found in Poland, and this suggested the system was unsafe.[22A] However, Mettig came into OKH SIGINT sometime after these events, and he is vague on some details; hence these messages may have been captured with the Poles in Czechoslovakia.[22B]

The Czechs had no liaison with the Polish bureau, but they had had good relations with the French cryptanalytic people, and possibly knew something from that source of French activity on the ENIGMA problem.[23]

The captured Poles stated during interrogation that they had worked on the machine with the French, and had the instructions for its use,

but the Germans were unable to discover exactly what had been done.[24] German investigators did discover that the Poles had possessed a section of extraordinary security in the Warsaw Cryptanalytic Bureau.[25] OKH knew that captured Polish secret documents contained decrypts of German cipher messages.[26] This started a rumor that the Poles had been reading the ENIGMA.[27] Further captured documents showed that the salaries of two mathematical students from Posen were exceptionally large, and this suggested that they had been successful in reading the ENIGMA.[28] The Germans had learned that the leading workers on this project were young Polish mathematics students, and apparently two such students were captured in Warsaw in 1939, but later neither could be found.[29] The Germans then calmed down.[30]

As a precaution they did some further studies on ENIGMA and concluded that the system for doubly enciphering the message setting and sending it as an indicator was a weakness because in some special cases the keys could be recovered.[31] They did not think the Poles were able to do this kind of attack, however, because "either a special deciphering machine was required, or a lengthy Hollerith operation. . . At that time it appeared doubtful that the Poles had carried out so great a task. . ."[32] To improve security, ENIGMA procedures for sending indicators were tightened at the beginning of 1940.[33] Outright solution of the ENIGMA was derided,[34] but as a precaution, the stecker plugging was increased from six to ten pairs at this time.[35]

In 1940, after the Battle of France, the Germans searched for further evidence of French success on ENIGMA in Belgium or France, but were never able to find any.[36] No cryptanalysts were captured, and all their papers were destroyed.[37] Files in the French Admiralty showed that British experts had come to France to help the French cryptanalysts on the Naval ENIGMA, but that neither cryptanalytic service had any success.[38] OKM (Oberkommando der Marine, Navy High Command) probably told OKW nothing of this British party.[39] Fenner of OKW saw a captured French document of an unknown source, urging that a "new bureau should be set up."[40] The files of the Deuxieme Bureau in Paris were searched, but they had been removed by the French to Vichy. A few documents were found in the Deuxieme Bureau showing that the French had succeeded about 1931–33 in buying information about German double transposition keys from a man working in OKW.[41] The Germans knew nothing about this until the documents were found, and never traced the man.[42] Nothing revealed ENIGMA success.[43] When Vichy France was occupied in late 1942, the Germans were busy with other matters, and

no search was made for a French cryptanalytic section, according to Hüttenhain of OKW.|44| The French cryptanalyst Bertrand *was* arrested and interrogated at this time, but he did not disclose the ENIGMA work, and it is very likely that he did not know what was happening in England and America on the problem.|45,46| Some Polish ENIGMA cryptanalysts fleeing to Spain were apparently captured at the border and imprisoned, but were not identified or interrogated.|47|

In 1940, after the fall of France, the Germans arrested a pair of Polish officers who had fled to France, but did not discover that they had held senior positions in the Warsaw cryptanalytic bureau.|48| Mettig claimed that many interrogations of Poles were held, but drew blanks.|48A| Some interrogations in 1942 were held in Warsaw,|48B| and in September 1942 an interrogation was held in Berlin. Mettig claimed that one of the Poles was a Lt. Colonel, head of the Cryptanalytic Bureau.|48C| In 1942 and 1943 the Germans had found evidence that their teletype landlines were being tapped in Paris.|48D| They knew that the Polish underground was sending espionage information by radio from Warsaw from 1939 until 1944.|48E| They were also aware that Polish "radio agents" were operating in France, and in March 1943 captured some.|48F| Later, in 1944, they read numerous enciphered messages from Polish agents in Northern France.|48G| After they occupied Vichy France, they found signs of French SIGINT, and according to Flicke, they uncovered an organization in Marseille in August 1943 associated with the Deuxieme Bureau and disguised as "Service Radio Electrique de Securité Territoire" which had over 40 stations with 300 trained operators.|48H| In 1943 General Fellgiebel ordered the reinterrogation of Polish cryptanalysts to check further into Fall WICHER.|48I| Representatives of OKM as well as OKH were present at some of these interrogations.|48J|

In 1943-44 the two Polish officers captured in 1940 in France "volunteered" the information that the Poles had been reading ENIGMA for several years before the war.|49| The two officers, a Major and a Lt. Colonel, were at that time in a PW camp in Hamburg.|49| Dr. Pietsch of OKH, who had been present at interrogations in Warsaw and probably at Berlin, was sent to Hamburg to question them.|50| The accounts vary somewhat, for Buggisch of OKH claimed that the Poles willingly gave Pietsch the information they possessed, on the argument that "after so long a period the question of security seemed pointless even from a Polish point of view."|50| Mettig of OKH claimed that the Abwehr messed things up by allowing the Poles to be together for several days before they were interrogated, and this gave them a chance to correlate their stories. He said there were no results because the Poles would not talk.|51| Buggisch and Mettig both mentioned a Lt.

Colonel from the Warsaw Cryptanalytic Bureau; so they may have been talking about the same person.[51A]

Since Hamburg had been devastated by the RAF in July 1943, and a million inhabitants had fled, the Poles presumably knew that the Allies were still in the war, but they may not have known of the British connection (it was never mentioned by OKW or OKH in describing Fall WICHER and they probably never told OKM people about the Polish decrypts) and thought that all ENIGMA work had long ceased. There were many uncertainties resulting from this interview. The Polish officers had been heads of sections in Warsaw and they were sure that the German Army ENIGMA had been read in part for several years before 1939.[52] They knew that the Polish workers had gone to France after the fall of Poland, but were not certain whether the Polish cryptanalytic work on the ENIGMA had been continued on French soil.[53] The Polish officers could give no details of the method used.[54] They claimed that some sudden alteration was made by the Germans which made it impossible to continue reading the traffic, but were unsure of the date.[55] As a result of Menzer's studies the Germans had made a change in the ENIGMA itself in the late 1930's, from three stecker-pairs to six or seven stecker-pairs.[56] Then in 1940, they changed the indicator system.[57] Lacking a date, they could not determine which change had caused the alleged halt.[58] The prisoners gave the Polish covername "WICHER," confirming the Czechoslovakian incident. Pietsch "did not bother to get details of the Polish method,"[59] and brought back a rather hazy general story to OKW/Chi.[60] Other German cryptanalysts, who had already heard of the 1939 revelations, thought it had been bad usage giving depths, which had allowed the prewar reading, rather than the indicator system.[61] Because of the uncertainties, the Germans concluded that some ENIGMA traffic had been read years before, but did not think there was any current threat and did not pursue the matter.

The ENIGMA had been the subject of security studies during the 1920's, and the first Army ENIGMA was tested in 1927.[62] It was seen in use about 1931-32,[63] and after further studies at that time by Schroeder,[64] the steckered ENIGMA was standardized with 3 stecker-pairs.[65] Menzer took up the work and ENIGMA was improved in the late 1930's—after the Poles had broken in—by using six or seven stecker-pairs instead of only three stecker-pairs.[66] German mathematical studies and other work had shown that a depth of about 30 was needed to read the traffic, and the unknown stecker plugging would stand up to any attacks they knew.[66A] Apparently, after the initial scare of October 1939, the Germans satisfied themselves that only the indicator system had a weakness, and having corrected that,

had no further doubts. They also rationalized that the decrypted German messages captured in 1939—which were not disclosed to OKW—could have come from reading depths, rather than actual solution of the machine.[67] They were very sure that any attack on the machine would require a large Hollerith process.[67A] Even though an Allied prisoner of war in North Africa had disclosed that the British and Americans were working together "with a very large joint 'park' of Hollerith (punch-card) equipment," this PW interrogation was never followed up.[68] (Apparently the location Bletchley Park was transformed into the generic term "park" in reporting this.) Late in 1943 a German officer escaped in North Africa and said the Americans had a large deciphering organization with Hollerith equipment, but the Germans were unable to confirm this.[69] Since the senior German cryptographers were, after the war, still convinced that the ENIGMA was unbreakable, they may have been reluctant to consider that a handful of young Polish mathematics students could produce cryptanalytic results which experienced senior German cryptanalysts could not.

II. COMMENT

After the war, the German cryptanalysts used the argument that ENIGMA was unreadable to justify lack of success to Typex, even though they had captured several Typex machines—without the rotors—at Dunkirk.[70] They also claimed to have no knowledge at all of the existence of an Allied SIGINT effort against them, although they inferred some things from Yardley's book and wartime U.S. newspaper articles.[71] There is no evidence to show that they understood *how* a steckered ENIGMA could be read, for even when they did finally introduce the pluggable reflector, the Army found it too much trouble, it was mentioned in Naval traffic but never used, and the Luftwaffe used it incorrectly.[72]

Yet the fact remains that the Germans became increasingly suspicious that their ciphers were being read, but thought this was due to betrayal of the current keys.[73] As the war went on, they went to extraordinary lengths to improve all their ciphers, to tighten up radio security, to investigate all the people who could possibly come near the keys, and to spread the traffic out over so many keys that a capture or a betrayal could not compromise more than a small portion of their communications.[74] Some of these security techniques they learned from Allied cryptographic practice, and copied them.[75]

They analyzed their own military reverses for signs of cipher compromise. In the early part of the war, only Luftwaffe keys were being read to any extent, but this had little influence on the war in the major

theaters.[76] Until late 1942 the Germans had little reason to conclude that their ENIGMA traffic was being read, and except for Luftwaffe there was not much success, for there were no decisive military consequences.[77] In North Africa the crucial tactical intelligence came from the TA and low-level cryptanalysis of the 8th Army SIGINT people in the field.[78] Convoy information was read from Italian traffic until the Porpoise ENIGMA key was broken in mid-1942.[79] British prisoners could have told the Germans nothing conclusive. On the Russian front the Russians were unable to read ENIGMA, and so no prisoners from generals downward could have told them otherwise, and up until Stalingrad, the Russians were still suffering major military reverses.

In 1943 the German Navy lost its continuity on a number of major Allied systems,[80] and success on Naval ENIGMA soon led to devastating losses of U-boats.[81] The attacks on Rommels supplies, and the attacks on U-boats were fairly well covered by using aircraft to make sightings before the subs were attacked;[82] however, the cover doctrine was not followed perfectly on U-boat rendezvous. The Germans did examine rendezvous at sea over a period in 1943 and noted that between 3 and 11 August 1943 every one of their rendezvous had been visited by Allied forces, a marked change from the previous period.[83] The possibility of the ENIGMA's being broken was considered, but treated as only "tentative."[84] The Abwehr in August 1943 sent a report from a German agent working at a high position in the Navy Department in Washington, stating that the operational orders to the U-boats were being read currently.[85] Abwehr considered the agent their best in Washington.[86] OKM left the question unresolved, preferring to blame radar and treason.[87] The "uncovered" sinking of U It 22 and the tanker BRAKE at an Indian Ocean rendezvous on 11 March 1944 precipitated a cipher crisis, and led to the introduction of special settings on each U-boat.[88] In 1942 the 4th wheel modification was introduced in U-boats.[89] In 1942 and 1943 new and complicated "Stichwort" procedures (based on a codeword known only to an officer on the U-boat) were introduced, to offset the effects of pinches and captures of current keys.[90] OKM even conceded that the U-boat ciphers were almost certainly read for a short period in 1943, because of "uncovered" Allied attacks, but concluded that the ciphers were only readable if *all* the cipher material and the "Stichwort" were captured or pinched or betrayed.[91] The somewhat blind attempts to improve ENIGMA security against betrayal and capture did in fact make the cryptanalysts' work much harder. The Germans also improved the U-boats themselves with Schnorkels and better torpedos and ELINT equipment, so that they could resist countermeasures.[92] Finally, in 1944 they directed a young Lt. Frowein to study ENIGMA

security, and in a few months he produced a study showing the key could be broken on a crib of 50 letters. He received a decoration, and rotor changes were ordered—too late.[93]

While OKM apparently did not know about Fall WICHER and OKW did not know about the Abwehr (counter-intelligence) report from Washington (owing to a Führer directive of 1940, intended to keep knowledge from those who needed it),[94] there were still a number of technical changes under development, any one of which could have finished off the cryptanalysis of the ENIGMA. The Luftwaffe had developed a pluggable reflector D, but could not get it adopted;[95] the Navy planned to use it in 1942, but never introduced it;[96] and the Army considered it too much trouble.[97] The Luftwaffe did introduce it, but used it wrongly, and it was solved.[98] The Army then used it correctly late in the war, but only on one key.[99] The Luftwaffe then introduced the ENIGMA Uhr (a dial switch yielding a multiplicity of steckers) to spread out the traffic on the steckers, but misused that too, and it was solved.[99A] The SG-39 designed by Menzer was still bogged down in development; so Menzer created the *Lückenfüllerwalze* (settable notch ring),[100] and this was tooled up and ready for production at Heimsoeth & Rinke in February 1943,[101] but decisions were put off because the ENIGMA was still considered secure. At security conferences conducted by General Gimmler from November 1944 to January 1945, "worry was expressed over the fact that the military machine had not been changed throughout the war."[102] The Germans had learned from documents in October 1942 that British Naval units would use *Typex* with 10 rotors for inter-service working, and additional sets of seven more rotors for Naval Code and seven rotors for Naval cipher, and even intended rotors with variable plugging for extra security.[103] At the Gimmler conferences, the OKL (Oberkommando der Luftwaffe, Air Force High Command) Uhr was discussed, the *Lückenfüllerwalze* was approved.[104] *Lückenfüllerwalzen* were ordered in a quantity of 12,000 and these were nearing completion at the ERTEL plant when the war ended.[105] Two more of Menzer's devices were ordered, viz., 20,000 *Schlüsselscheiben* and 70,000 *Schlüsselkasten* were ordered in early 1945 to replace ENIGMA, and 15 toolmakers were committed to expedite the project.[106]

Some useful insight into the German attitude toward ENIGMA security can be gleaned from noting the actions taken by the Germans themselves, which connote something different from their postwar statements. In 1942 Pers Z (Foreign Office) approached Willi Korn of Heimsoeth & Rinke and discussed the construction of a six-rotor ENIGMA-compatible cipher machine called SG-42, which apparently never passed theoretical development.[106A] At the time of the Allied

landing in North Africa in late 1942, General Martini, Chief Signal Officer of the Luftwaffe, stated that the ENIGMA was "only 80 percent secure" (whatever that means) and banned the transmission of operational orders by radio.[106B] (An undersea cable to North Africa was installed for Rommel's operational orders.[106C] OKL SIGINT people in Northern Italy in 1943 were ordered to send secret or top secret information over cipher teleprinter. ENIGMA was to be used only in exceptional cases.[106D] To increase the cryptographic security of ENIGMA for OKL SIGINT traffic, different machine settings (keys) were used on successive messages without external indications. [106E] Allied bombing of landlines forced the use of radio, but the D-reflector (pluggable) was used in 1944 for "especially important messages," after which the standard reflector was put back into the machine for routine messages.[106F] An OKL technical sergeant stated that in SIGINT reports, "codewords were substituted for numerical designation of Allied units. . .to partially veil the results of German Signal Intelligence in the event that ENIGMA messages were being deciphered by the enemy."[106G]

Information in a captured OKH war diary is also revealing. In March 1944, OKH was studying a new system for assigning and enciphering callsigns.[106H] Studies were instituted to determine the extent to which Army ENIGMA could be compromised by *treachery*, and it was noted that "retaining the present key techniques, five message keys chosen by specific agreement are sufficient to betray the daily key without permitting the German control agency to spot the betrayal, even with careful checking."[106I] The Germans strongly suspected that one or more ENIGMA cipher clerks was choosing settings in a way that Allied SIGINT, by prearrangement, could exploit to break the key. OKH studied the "betrayal" problem, and OKH also studied the Navy ENIGMA procedures and pronounced them "totally inadequate from the point of view of security. . . A general solution for compromise cases with the steckered ENIGMA by means of an extensive cryptanalytic auxilliary device was found." Even the Army ENIGMA was thought vulnerable to depths of four messages, "by using an extensive system of mechanical cryptanalytic aids."[106J]

The stress in the OKH war diary on special machinery and betrayal strongly suggests that they had more than an inkling of the huge machine attacks currently being carried out in England and in the United States.

The war diary subsequently noted that several reports on the ENIGMA were done in 1944, and in October 1944 OKH recorded that work had been concluded on the compromise problem of the plugged ENIGMA. The *Schlüsselkasten* studies were mentioned, and the new

system for enciphered callsigns was scheduled for introduction on 1 September 1944. Production of ENIGMA Uhr was noted.[106K]

The occurrence of many cryptographic technical matters in the OKH war diary indicates that the upper levels of OKH were very sensitive about their cipher security. German hand systems were also systematically tightened up, and it was noted in late 1944 by Allied SIGINT that they had become so secure that it was necessary to solve high-grade ciphers (Fish or ENIGMA) to obtain cribs to solve the medium-grade hand ciphers (raster).[106L] Captured papers belonging to the OKW mathematician Hüttenhain note that in September 1944 OKW was engaged in security improvements to the stencil system, developing emergency keys for the stencil system in case of capture, and production of a new emergency system for ENIGMA (usage). New cipher instructions for ENIGMA were to be published, and a new manual for ENIGMA was also expected.[106M] In addition, they were investigating the production of keys for ENIGMA equipped with *Lückenfüllerwalzen.*[106N] All of this activity suggests a significant change in German cryptographic thinking.

Among the captured Hüttenhain papers were notes on security lectures given by Leutnant General Gimmler, OKW/Chef Ag WNV, who was charged with coordinating all Armed Forces cryptographic security studies. In his lectures emphasizing the preservation of signals security by technical means, he stressed the activities of foreign SIGINT several times, viz:

> "In the years after the War, the world learned what the enemy had been able to obtain from deciphered messages, to the detriment of Germany. The enemy's cryptanalytic work has been further developed.
>
> "The British possess an admirably trained political and military Sigint service. In the First World War, the Americans were, in this respect, positively naive, but they learnt from the British, and now work on cryptanalysis, for example, with the assistance of the most modern mechanical devices. Similarly the Bolshevists . . . have tapped our tactical and operational signals communications sometimes close to the front, sometimes far in the rear area, and have retransmitted the contents by agents' W/T.
>
> "Sigint successes (German) in Italy and during the battle of Normandy have been dazzling even to the expert. . . Today, cryptanalysis is breaking complicated speech encipherment systems and difficult hand and machine systems without a knowledge of the keys. . . The Sigint and crypto battle is fought just as bitterly in this war as the battle with weapons.
>
> ". . . no secure method of speech encipherment exists. . .the most secure method is to entrust top secret material (geheime Reichsachen and Chef-und geheime Kommandosachen) to a reliable courier or to the cipher teleprinter."[106O]

Allowing for the "pep-talk" character of his lectures, Gimmler's reference to the American use of "most modern mechanical devices"

for cryptanalysis, and his assertion that the cipher teleprinter was the "most secure" method of transmission, again raise the same points, viz., that new, special machinery was being used for Allied cryptanalysis, that ENIGMA could be attacked by such machines, but that the Fish teleprinter was still secure.

Because the OKH SIGINT organization "dissolved" at the end of the war before the TICOM groups could find the people, equipment or documents, much less is known about OKH work than is known of OKL and OKM and some of the other cryptologic agencies.[106P] Since it is known that Gehlen sent his Army Intelligence organization into hiding at the end of the war, and hid multiple copies of all his vital records on the Russian forces, it is not beyond belief that OKH SIGINT carried out some "phoenix" plan.[106Q] The postwar statements of OKH and OKW higher-ups uniformly claimed that the ENIGMA was unbreakable, but the captured war diary and other documents, and the statements of people lower down don't show the same confidence.

In 1943 the Germans removed all discriminants from the traffic and in 1945 they introduced unsolvable enciphered callsigns.[107] In Italy alone they had 11 different keys concurrently in use.[108] They avoided the use of radio; Rommel had a submarine cable between North Africa and Italy, and landline was used everywhere possible.[109] Their hand ciphers were systematically analyzed and improved.[110] They printed and distributed tons of cryptographic materials late in the war, to improve signal security, even below division level.[111] Important information was kept off radio; for the 1944 Ardennes offensive, radio silence was supplemented by the use of couriers for the operational orders.[112]

In similar circumstances, when the British Navy found in 1942-43 that its codes and ciphers were being read, they were reluctantly changed.[113] After they captured the German Long Range Signal Reconnaissance Company No. 621 at Bardia in North Africa in 1942, the British Army changed all their systems.[114] After the discovery that the U.S. Attaché's messages from Cairo to Washington had been exploited to Rommel's advantage, the U.S. gave the Attaché a cipher machine.[115] Generally it takes a shock to bring about a change to a completely new cipher system.[116]

After the war, when the reconstituted West German Government established its cryptography, the ENIGMA was *not* brought back into service. Instead, the Foreign Office adopted the T&N (Telephonbau und Normalzeit) machine--a development from Menzer's original SG-39, but much more secure.

The intensive efforts that the Germans made to improve cipher and traffic security coincided roughly with the increasing buildup of

Allied SIGINT against them.[117] Although the Germans denied any knowledge of this vast Allied SIGINT effort, there were thousands of people in Britain and the U.S., and in the Mediterranean and European Theaters who knew that SIGINT was a big effort and who also knew that German high-level signals were being read. Some of the aircrews operating over Europe, and shot down there, may have known more than they were supposed to. What almost no one knew, except for a very small handful of cryptanalysts and intelligence analysts, was the *details*, viz., which links, which keys, how it was being done, how current the decrypts were, and what intelligence they contained.[118]

The Germans acted, from 1943 onwards, as if they *knew* that a large mechanized Allied SIGINT effort was directed against ENIGMA, but clearly believed the "Fish" cipher teleprinters were completely secure—which they were not. This suggests some kind of incomplete leak, possibly from gossip from people who knew that ENIGMA was being exploited, but did not know about "Fish" exploitation. A leak of this kind could have occurred from the lower levels of Allied cryptanalytic processing, where thousands of people were employed, or it could have occurred from high levels above the cryptanalytic organizations, or from consumers who had been told about ENIGMA exploitation, but not of the other sources for Special Intelligence.

The increasing cryptographic changes and innovations by the Germans suggest that they had increasing suspicions, possibly knowledge, from espionage or prisoners or even SIGINT on Allied or neutral systems, that their traffic *was* being read, but not *how*.[119] (There are apocryphal stories of Washington cab drivers in World War II knowing where the "code breaking" centers were, and with 13,000 SIGINT workers in the two cryptanalytic centers, it would be surprising if the Germans knew nothing.) The Germans may have supposed that traitors were betraying the daily keys (after the Paris discoveries), but because they never made the simple changes which *would* have made the traffic unreadable, they apparently never discovered the truth.[120]

Because ENIGMA continued to be exploited through the war, it was easy to suppose that the Germans did not know it was being read, and the postwar TICOM interrogations seemed to confirm this. However, the interrogations may have been less revealing than other evidence. Because the Germans did not replace ENIGMA, there is a tendency for Allied security doctrine—based largely on wartime doctrine—[120A] to be accepted uncritically as a correct scheme for preserving cryptanalytic successes. The central point of this doctrine—that *any* enemy knowledge of a SIGINT success will destroy that success—is not confirmed by the WICHER affair. The converse proposition—that continued success meant that security doctrine was both correct and

effective—is also questionable as well as being a *non sequitur*. Hence, Fall WICHER is not irrevelant to the analysis of security and operational problems of today.

The central issue in Fall WICHER was that, although the most useful people and resources were evacuated from Warsaw, the coverup was not *complete* and it was not well thought out. Some of the records were destroyed before Warsaw fell, some fell into German hands. For unexplained reasons, the WICHER people left behind in Warsaw travelled as a *group* into Czechoslovakia, which had been occupied by the Germans in March 1939, carrying with them a quantity of secret records containing decrypts. No doubt the Russian advance cut them off from direct access to Rumania, but with the documents they could hardly pose as refugees. When they were caught, the interrogators had a homogeneous party *and* their records to pursue in the investigation, and the essential fact—that ENIGMA was being read—was exposed. The 1940 operation in France let knowledgeable people who had fled Poland fall into German hands, and eventually they confirmed the earlier disclosures. Even the Mission Richard party had to leave France without much preparation in 1940. The operation in Vichy France by Bertrand had no contingency plan for evacuating the people, and a number of them were arrested, fortunately before the Hamburg disclosures. The security compartmentation and the rather abstract mathematical nature of the cryptanalysis were apparently critical factors which kept the Germans from getting the specific details they needed, because the people who did talk didn't know them. Yet the continued success on ENIGMA—quite important during the 1943-45 period—was hanging by a very slender thread. If the Germans had interrogated a few more people, or had made better use of the information they did receive, the Allied SIGINT position might have been very different, and the war itself might have been very different.

III. REFERENCES

Note: S documents are mostly TICOM; *NS* = GCCS Naval SIGINT; *AS* = GCCS Army and Air Force SIGINT; *AH* = GCCS Army and Air Force History; *C* = NSA Cryptologic Library in P1.

[1] S-4836 (TICOM/I-176), *Homework by Wachtmeister Dr. Otto Buggisch of OKH/Chi and OKW/Chi* (November 1945), p. 11; *Naval Sigint*, VII, 157.

[2] S-4589 (TICOM/I-92), *Final Interrogation of Wachtmeister Dr. Otto Buggisch* (25 August 1945).

[3] *Ibid.*; *NS*, VII, 161-169.

[4] S-4860 (TICOM/I-200), *Interrogation of Min. Rat Wilhelm Fenner of OKW/Chi* (September-October 1946).

[5] S-4836; S-4860.

[6] Brigadier Peter Young, *Atlas of the Second World War* (G. P. Putnam, New York, 1974), pp. 16–17.
[7] *Ibid.*
[8] Information from John H. Tiltman.
[9] S-4862 (TICOM/I-202), *Interrogation of Min. Rat Victor Wendland of OKW/Chi* (September 1946).
[10] S-4860.
[11] S-4862. (*Note:* The Czechs did not read ENIGMA, although some German SIGINT people thought they had claimed to. *Naval Sigint*, VII, 157, is unmeticulous on this point.)
[12] S-4860, p. 2.
[12A] S-4578 (TICOM/I-78), *History and Achievements of the Cryptographic Section of the OKH* (August 1945); S-4782 (TICOM/I-142), Barthel, *OKH*. There is no indication in TICOM that OKH ever told OKW or anyone else about this; it seems to have been virtually forgotten.
[12B] S-4862.
[12C] S-4860, p. 11.
[12D] S-4782 (TICOM/I-142), *P/W Barthel's Account of German Work on British, American, Swedish and French Machine Ciphers* (October 1945).
[13] S-4860.
[14] S-4860, p. 2.
[15] S-4532 (TICOM/I-31), *Detailed Interrogations of Dr. Hüttenhain, Formerly Head of Research Section of OKW/Chi* (June 1945).
[16] S-4860, p. 2.
[17] *Ibid.*
[18] S-4860, pp. 10f.
[19] *Ibid.*
[20] *Ibid.*
[21] S-4165 (TICOM/DF/234-A), *ENIGMA Files 1924–44*, p. 18; S-4584, (TICOM/I-84), *Further Interrogation of Dr. Hüttenhain and Dr. Fricke of OKW/Chi* (August 1945).
[22] S-4860, p. 11.
[22A] S-4767 (TICOM/I-127), *Interrogation of Oberstlt. Mettig of OKW/Chi* (September 1945); S-4578.
[22B] S-4578.
[23] S-4860, p. 2.
[24] S 4532; S-4860.
[25] S-4589 (TICOM/I-92), *Final Interrogation of Wachtmeister Otto Buggisch* (August 1945).
[26] S-4836.
[27] *Ibid.*
[28] *Ibid.*
[29] S-4589; S-4836.
[30] S-4836.
[31] S-4836; *AS* VII, p. 58; S-4589, p. 5.
[32] S-4589, p. 5; S-4836, p. 11.
[33] S 4836, p. 11.
[34] S-4589, p. 5.
[35] *AS* VII, p. 59.
[36] S-4532.
[37] S-4860.
[38] *IR*-84052, *Naval Historical Team Report*, p. 21.

[39] S-4860, p. 3.
[40] S-4860.
[41] S-4860, p. 8.
[42] *Ibid.*
[43] S-4532.
[44] *Ibid.*
[45] Gustave Bertrand, *ENIGMA, ou la plus grande énigme de la guerre 1939-1945* (Librarie Plon, Paris, 1973).
[46] For a review of Bertrand's book, see Edwin S. Spiegelthal's "The Cryptologists Who (Briefly) Went Back Into the Cold." *NSA Technical Journal*, XIX, 3 (Summer 1974), 109-112.
[47] Information from John H. Tiltman.
[48] S-4836, p. 12.
[48A] S-4767.
[48B] *Ibid.*
[48C] *Ibid.*
[48D] S-4578, p. 11 (see reference 12A).
[48E] S-65,897, Wilhelm F. Flicke, *War Secrets in the Ether* (Trans. by R. W. Pettengill, NSA 1953). (Based on a MS by Flicke written from memory in 1945), pp. 245-248; S-2106, General A. Praun, *German Radio Intelligence* (1949-50) (Historical study of 1914-1945), p. 212.
[48F] S-2106, p. 204.
[48G] Flicke, pp. 245-248.
[48H] Flicke, p. 260.
[48I] S-4578.
[48J] S 4767.
[49] S-4836, p. 12.
[50] S-4836; S-4589, p. 6.
[51] S-4767.
[51A] S-4836; S-4767.
[52] S-4836, p. 12; S-4589.
[53] S-4589, p. 5; S-4836, p. 12.
[54] S-4836, p. 12.
[55] *Ibid.*
[56] S-4860, p. 12.
[57] S-4836.
[58] S-4589, p. 5.
[59] *Ibid.*
[60] S-4836, p. 12.
[61] S-4589, p. 5.
[62] S-4803 (TICOM/M-13), *Manufacture of ENIGMA Machines by Heimsoeth & Rinke, Berlin*, by Major Heller (October 1945).
[63] *NS*, VIII, 121.
[64] S-4862.
[65] S-4165, p. 18.
[66] S 4860.
[66A] S-4532, p. 15.
[67] S-4589, p. 5.
[67A] *Ibid.*
[68] S-4584.
[69] S-4860, p. 2; S-4866 (TICOM/I-206), *Extracts from Homework Written by Min. Rat Wilhelm Fenner of OKW/Chi* (pre-June 1945).

|70| S-4578 (see reference 12A); S-4558 (TICOM/I-58), *Interrogation of Dr. Otto Buggisch of OKW/Chi* (July 1945); S-33,656 TL, *TICOM Histories*, Vol. B, Part II, *Axis Cryptanalysis of United States Cryptographic Systems* (ASA, 16 August 1946). (No author, corrected or edited draft. This is not a TICOM document, but an account based in part on TICOM material and in part on apparent knowledge of U.S. cryptography. It may, therefore, not be definitive.)

|71| S-4584; S-4866.

|72| *AS*, VII, 89; *NS*, VIII, 21.

|73| *NS*, VII, 189-195, 202, 228-231; *AS*, VII, 71.

|74| *AS*, VII, 55f; S-4593; *NS*, VII, 13, 119.

|75| S-4511 (TICOM/T-12), *A Translation of the Preliminary Interrogation of Orr. Tranow of 4 SKL/III OKM Carried out at Flensburg on 24/24 May 45*, p. 10; S-4590 (TICOM/I-93), *Detailed Interrogations of Members of OKM* 4 SKL/III at Flensburg (June 1945), p. 16.

|76| *NS*, VIII, p. 139, p. 172.

|77| *NS*, VII, p. 170; *NS*, IV, p. 116.

|78| *AH*, IV, p. ii.

|79| *NS*, VIII, pp. 150-154, 280-282; *NS*, IX, 29-31; *NS*, IV, 158-163.

|80| *NS*, VII, Ch. VI.

|81| Edward von der Porten, *The German Navy in World War Two* (Ballantine, New York, 1974), Ch. 9.

|82| *NS*, IV, pp. 158-163; *NS*, VII, pp. 150-153, 210 213, 216-219.

|83| *NS*, VII, pp. 217f.

|84| *NS*, VII, pp. 197, 217f, 199, 175.

|85| *NS*, VII, p. 215.

|86| *Ibid.*

|87| *NS*, VII, p. 219.

|88| *NS*, VII, p. 222.

|89| *NS*, VII, p. 20.

|90| *NS*, VIII, pp. 16-19.

|91| *NS*, VII, pp. 166 169, 206-208, 218, 229; *NS*, VIII, pp. 12, 20.

|92| *NS*, VII, pp. 213, 231.

|93| *NS*, VII, p. 160; S-4592.

|94| S-65,897, Milton Shulman, *Defeat in the West* (Secker & Warburg, London 1947), pp. 14-20; S-65,897, Flicke, p. 234.

|95| S-4532.

|96| *NS*, VII, p. 21.

|97| S-4532.

|98| *AS*, VII, pp. 71-73, 89.

|99| *AH*, V, 24; *AS*, VII, 89.

|99A| *AS*, VII, 73f.

|100| S-2636 (TICOM/DF-174-A), *Four Papers by Fritz Menzer* (Pre-1949).

|101| S-4166 (TICOM/DF 239-B), *ENIGMA Files (Patents) 1931-43*; S-4521 (TICOM/I-20), *Interrogation of Sonderführer Dr. Fricke of OKW/Chi* (June 1945); S-4777 (TICOM/I-137), *Final Report Written by Wachtmeister Otto Buggisch of OKH/Chi and OKW/Chi* ((a) SG-39, (b) Hollerith and special machinery in the solution of Hagelin traffic, October 1945).

|102| S-4589.

|103| S 3191 (TICOM/D-43); TICOM/T-520), *Translation of Four Cryptanalytic Reports by OKM/4/SKL/III on Allied Naval Systems* (from a folder entitled "Research Progress 30 November 1944-21 March 1945").

|104| S-4589.

[105] S-4847 (TICOM/I-187), *Report on Production of ENIGMA Cipher Machines by the Ertel Factory, Hohenaschau* (September 1945).
[106] S-4593 (TICOM/I-96), *The Activities and Organization of the Cipher Department of the Armed Forces (OKW/Chi)* (August 1945).
[106A] S-3116 (TICOM/D-3L), *Conversation with Engineer Korn (ENIGMA Cipher Machine Factory, Schauffler & Houthal)* (23 February 1942; S-3115 (TICOM/D-3K), *Machine 42* (SG-42) (21 February 1942).
[106B] S-61,466 (TICOM/IF-5), *Notes on Field Interrogation of Various German Army and Air Force SIGINT Personnel* (May 1945), 11 pp.
[106C] S-4860, p. 7.
[106D] S-5621 (IF-184), *Seaborne Report, The Signal Intelligence Service of the German Luftwaffe*, Vol. IX, *History of Operations in the South* (USAFSS 1951), 72.
[106E] *Ibid.*, pp. 73f.
[106F] *Ibid.*
[106G] *Ibid.*
[106H] S-4227 (TICOM/DF-300), *War Diary of the Signal Intelligence Group* (From the OKH War Diary, February-November 1944), p. 21.
[106I] *Ibid.*, pp. 22, 39.
[106J] *Ibid.*, p. 40.
[106K] *Ibid.*, pp. 47-48, 64, 69, 99.
[106L] Letter by A. Small at GCCS to CO, SSA, War Department, 27 December 1944, referring to a report by Prof. Vincent at GCCS (in the *Pettengill Papers* -or Goldner notes).
[106M] S-3220 (TICOM/D-68), *Further Miscellaneous Papers from a file of R. R. Dr. Huttenhain of OKW/Chi*, 23 July 1944-20 December 1944 (incl. Gimmler lecture notes).
[106N] *Ibid.*
[106O] *Ibid.*
[106P] S-4763, TICOM (EUXIS), *European Axis Signal Intelligence in World War II as Revealed by TICOM Investigations and by Other Prisoner of War Interrogations and Captured Materials* (May 1946), p. 78f; Vol. VIII.
[106Q] E. H. Cookridge, *Gehlen: Spy of the Century* (Hodder & Stroughton, London 1971), pp. 102-123.
[107] *AS*, VII, 85, 89.
[108] *AH*, V, 22.
[109] S-4860, p. 7.
[110] *AS*, VII, pp. 96, 99, 102, 108, 129, 132-133.
[111] S-4593; *AS*, VII, 86.
[112] *AS*, VII, 76-78; Milton Shulman, *Defeat in the West* (Secker & Warburg, London, 1947), pp. 15, 229f.
[113] Donald McLachlan, *Room 39* (Atheneum, New York, 1968), pp. 76-80; *NS*.
[114] S-4865 (TICOM/I-205), *Detailed Interrogation Report of former Regierungsbaurat Johannes Anton Marquart of OKH/GEN d. NA* (June 1947).
[115] S-4860, p. 12; probably SIGFOY.
[116] *NS*, VII, 222, 230.
[117] *AS*, VII, 69-74; *AS*, I, 253-256.
[118] *NS*, VII, 228f.
[119] *Ibid.*, 160-162, 209.
[120] *NS*, VIII, 12; *NS*, VII, 225; *AS*, VII, 86.

[121] S-4137 (TICOM/DF-202), Wilhelm Fenner, *The History of the Cryptologic Agency* (1945); *Military Cryptanalysis* II, 545. The patent application was filed in Germany 23 February 1918, German Patent No. 416,219. Koch filed a patent for ENIGMA with reflector in Holland in October 1919, No. 10700.
[122] C-1183 (TICOM/DF-213), Ing. A. Scherbius, *Radio Telegraphy and Cryptography* (1923).
[123] C1249 (TICOM/DF-218), *"ENIGMA" Cipher Machines* (1923).
[124] S-4137; S-4165. The Cryptologic Bureau was founded in 1920 as part of the Abwehr, but was funded by a registered club, Nuntia, which got its money from German heavy industry, but this was under Abwehrgruppe's direction. Later the Army procured it. They had cryptographic responsibilities, collaborated closely with Chiffriermaschinen, A. G., which was a corporation set up in 1923 by German business men to develop ENIGMA. Part of the ENIGMA was developed by the Cryptologic Bureau, and the German government owned some rights and imposed secrecy regulations on parts of the ENIGMA machines and on its sale and distribution during the 1920's and after.
[125] S-4165; S-4584.
[126] S-4165, p. 5.
[127] S-4584; S-4165, p. 9.
[128] C-1048, *U.S. Patents for ENIGMA Ciphering Machines* (n. d., pre-1953).
[129] S-4165, p. 16.
[130] *Ibid.*, p. 18; S-4137.
[131] S-4165, p. 24; S-4803.
[132] S-4165, pp. 11, 32.
[133] *Ibid.*, pp. 11, 15, 17.
[134] *Ibid.*, p. 18.
[135] *Ibid.*, pp. 18-24.
[136] S-4803.
[137] S-4803; *NS*, VIII, 121.
[138] S-4165, p. 32.
[139] S-4860, p. 12.
[140] S-4862.
[141] *Ibid.*, S-4860, p. 12.
[142] *AS*, VII, 59.
[143] *Ibid.*
[144] *NS*, VIII, 10.
[145] S-4803.
[146] *Ibid.*
[147] *Ibid.*
[148] *Ibid.*
[149] *Ibid.*
[150] S-4521; *NS*, VIII, 121.
[151] S-4803.
[152] S-4584.
[153] S-4165, p. 45.
[153A] C-1318, Willi Korn, *Permutating Device for Use in Coding Machines*, U.S. Patent No. 1,705,641, March 1929.
[154] *NS*, VIII, 121.
[155] *Ibid.*
[156] *Ibid.*
[157] *Ibid.*
[158] *NS*, VIII, 122.

[159] *Ibid.*, 121f.
[160] *AS*, VII, 58.
[161] *NS*, VIII, 122-127.
[162] *AS*, VII, 58.
[163] *Ibid.*, p. 59.
[164] S-4836.
[165] *AS*, VII, 59.
[166] *NS*, VII, 124.
[167] Bertrand, *ENIGMA*, *op. cit.*
[168] *NS*, VII, 122.
[169] S-4521; *NS*, VII, 122.
[170] *NS*, VII, 20.
[171] S-4521.
[172] *NS*, VII, 174f., 166-169.
[173] *AS*, VII, 51.
[174] *Ibid.*, p. 50.
[175] *Ibid.*, p. 42.
[176] *Ibid.*, pp. 41-44.
[177] *Ibid.*, pp. 42, 46.
[178] *Ibid.*, pp. 40-42.
[179] *Ibid.*, p. 49.
[180] *Ibid.*, p. 77.
[181] *AS*, VIII, 190.
[182] *Ibid.*, pp. 47, 190.
[183] *Ibid.*, p. 190.
[184] *Ibid.*, p. 140.
[185] *AS*, VII, 48.
[186] *AS*, XII, 295.
[187] *AS*, VIII, 210.
[188] *AS*, VIII, 142f.
[189] See reference 106L.
[190] *AS*, III, 21f.
[191] *AS*, II, 162.
[192] B. Page, D. Leitch, P. Knightley. *Philby* (Andre Deutsch, London, 1968), pp. 138f., 149, 156.
[193] S-2106, Praun, *German Radio Intelligence*, pp. 200, 211, 217; S-3220 (Gimmler lecture). TICOM/D-68. See 106M.
[194] *AS*, VII, 32, 141-143.

Appendix A: Prewar ENIGMA Communications Security and Cryptanalysis

The ENIGMA had been developed and subjected to theoretical security studies from the early 1920's. Dr. Scherbius of the Army High Command originated the wired rotor machine in World War I,|121| and became a principal of a company, Chiffriermaschinen A.G., Berlin, which in 1923 was advertising a four-wheel rotor machine called "ENIGMA" with 28-point wheels and automatic printing.|122| A company brochure gave an analysis of ENIGMA security, and Scherbius published a paper on the subject in 1923.|123| This company was closely associated with the German Defense establishment.|124| Later it was superseded by Heimsoeth & Rinke of Berlin, who controlled the patents but did not manufacture the machine.|125| The German Foreign Office objected to the fact that the 28-point ENIGMA needed line current, and might malfunction, and refused to adopt it.|126| What the military wanted was a rugged, compact machine which could be used in mobile warfare. A manually operated battery-powered machine, referred to as the "lamp panel ENIGMA" was developed by Dipl. Ing. Willi Korn.|127| U.S. Patent applications by Korn date back to 1926.|128| Correspondence from Heimsoeth & Rinke files show that the German Navy ordered 50 lamp-panel machines of the 1924 model (which had 29 letters) in late 1925.|129| Security studies had shown weaknesses, and Fenner of the OKW/Chi was involved with Korn of H & R in the 1926-31 period in the development of a steckered ENIGMA.|130| The 1923 printing ENIGMA was bulky, heavy and complicated. Korn had developed a rugged, simple and extremely reliable machine, which could be manufactured in quantity. The unsteckered version was adopted, and in 1927 the Army received 400.|131| German Signal Corps assumed this unsteckered battery ENIGMA in their planning, and the equipment installations in mobile communication vehicles left sufficient physical space only for that machine; when a steckered version of ENIGMA was required, the case could not be made larger except to lengthen it by 5 cm., and this physical limitation—and the German insistence on compatibility of equipment with the existing "system"—made it very difficult for them to include more rotors or more pluggings in the machine.|132| Attempts were made to install a 26-point stecker in the existing case, but this was not compact.|133| As a result, stecker-pair plugs were introduced to provide a compact partial plugging on the front of the machine.|134| OKW insisted this development be kept secret; this was in early 1928.|135| The Army ordered hundreds more of these 26-point battery-ENIGMAs, and had about 600 in service in 1930.|136|

The Navy continued to use the older ENIGMA with 28-point wheels (which had a 29th letter self-encipher bypassing the maze) until 1934 when they also obtained 401 of the three-wheel lamp-ENIGMAs using 26-point rotors.[137]

In 1929 a pluggable reflector was proposed by H&R, but was rejected by Fenner and others of the Cryptologic Agency.[138] The early models of the steckered-ENIGMA, which reportedly came into service in 1931, used only 3 stecker-pairs as variables, the other letters being fixed.[139] A Dr. Schroeder of the Cryptanalytic Agency first made an examination of the lamp-ENIGMA in 1932-33.[140] Later, Menzer, who was detailed to the Cryptanalytic Agency in 1934 from the Army, took up the work and the ENIGMA was improved by the use of more changeable stecker-pairs, viz., six pairs.[141] This was apparently done about 1935. Later, in early 1940, as part of the Fall WICHER security review, a change to 10 stecker-pairs was made, so that only six letters were unsteckered.[142] This 1940 stecker change was accompanied by an indicator change.[143] The German Navy cipher doctrine was to provide the highest security for the combat vessels, minesweepers, U-boats, etc., and they assumed captures would occur; so the strength of the machine was intended to lie in the variable stecker, which was considered unbreakable.[144]

Manufacture of the battery-ENIGMA was substantial.[145] By 1930 the German Army had 586. By 1939 they had over 10,000, and some 20,000 three-wheel steckered Army ENIGMAs were produced by the end of the war.[146] The Navy adopted it in 1934 with an order of 401, and by 1939 had 1500.[147] By the end of the war some 8500 three-wheel ENIGMAs had been produced for the Navy under H & R auspices, and another firm, Geyer, had 3000 serial numbers for Naval ENIGMA.[148] The total number of standard ENIGMAs was probably over 30,000[149] All these ENIGMAs had the same wirings for three rotors, and later for five rotors.[150] A smaller number of special ENIGMAs was also produced for special users.[151] Particular users, such as Hitler's train, had their own unique wirings.[152] During the war the manufacture of the K and G model ENIGMA was discontinued.[153] Multiple-notch rotors were patented in the United States in 1933.[153A]

While the Germans were systematically improving and testing the ENIGMA, and putting it into wide service, the Poles were attacking it by cryptanalysis.[154] The 29-letter Naval ENIGMA used in the 1920-31 period was worked on and read by the Poles starting about 1920.[155] Presumably German ships in the Baltic provided them traffic. In 1931 the 26-letter Heimsoeth & Rinke three-wheel ENIGMA was found to be in service (possibly the Army machines in

the 1927-31 period were not used for radio traffic until the stecker modification was available).[156] When Naval use of the three-wheel ENIGMA started (about 1935) there were only three rotors, and only six stecker-pairs were plugged up; so 14 letters were unsteckered.[157] The Poles obtained a photograph of the keys for a three-month period, during which time the wheel order did not change, and from this recovered the wirings of all three wheels by cryptanalysis.[158]

At this time the indicator system was weak, the so-called "throw-on" system in which the operator chose a window setting and enciphered it twice, starting with the machine at a fixed "grund" (basic) setting.[159] The resulting hexagraph was sent as the indicator. The indicator system was then changed, and the accounts vary somewhat. In Army usage the operator chose a grund and a setting, then sent the grund in the clear and doubly enciphered the setting as before, resulting in a 9-letter indicator but not curing the "throw-on" weakness.[160] C.H.O'D. Alexander, in the *Naval Sigint* history states that the Navy indicators changed on 1 May 1937 to a digraphic indicator encipherment, and that it was very hard for the Poles to overcome this, although they finally got into the new period by a crib.[161] The *Army and Air Force Sigint* account states that the fixed grund continued until the end of 1938, and then went to the variable grund.[162] Presumably the German Navy did things differently than the German Army. The Army account states that in April 1940 the Germans went to a new indicator system with an operator-chosen grund, and an operator-chosen setting, in which the grund was sent in the clear, but the setting was enciphered only once. The resulting six-letter indicator did *not* have the "throw-on" property, which made attacks on the machine much harder.[163] The German OKW people stated after the war that they corrected the double-encipherment weakness with a new indicator system at the start of 1940, and here the dates agree.[164] The *Army and Air Force Sigint* account states that the Germans also went to 10 stecker-pair pluggings at the start of 1940, and the *Naval Sigint* story mentions this too, but the German OKW TICOM interviews never mention this fact (which is less obvious than an indicator change).[165]

Because of the indicator changes, after 1937 the Poles found it much harder to read Naval messages, though they managed to do so by some cribbing and by using their Bombe.[166] The French supplied the Poles with some pinched materials, and they managed to read some ENIGMA traffic up to the outbreak of the war.[167]

The Germans, in addition to stecker modifications and indicator changes, distributed more rotors. In the Naval ENIGMA, wheels 4 and 5 had been introduced by December 1938.[168] Then wheels 6 and 7 were introduced (and captured by early 1940).[169] The Navy

also developed a new reflector wheel which allowed a fourth wheel to be placed in the existing 3-wheel ENIGMA, and this came into service in early 1942.[170] The Army and Luftwaffe added two more wheels to their ensembles.[171]

Because of the long development of the ENIGMA, and the many security studies, the German cryptanalysts were fully confident that the ENIGMA was secure if it was properly used.[172] However, the military services did not allow the cryptanalytic bureaus to monitor real German traffic, and so they were unaware of the extent to which operators' habits, stereotyped messages and other clichés had created weaknesses in the traffic.[172] Their security investigation in the WICHER case was based on a hypothetical usage of the machine. The Poles, after almost 18 years of reading German traffic, had a much more accurate knowledge of ENIGMA usage than the OKW cryptanalysts, but the Germans never discovered this.

Appendix B: Security of Fish Successes vs. ENIGMA Successes

The complete faith which the Germans expressed about the Army "Fish" cipher teleprinter strongly indicates that they got no leaks or espionage reports on TUNNY exploitation comparable to Fall WICHER. The Germans were apparently sensitive to capture, for soon after an OKL STURGEON cipher teleprinter (SZ-52) was captured in North Africa they forbad the sending of secret or top secret information on STURGEON, and warned that enemy decipherment was possible.[174] Their security studies of TUNNY showed some of its weaknesses, but not all.[175] They were fearful of cryptanalysts on STURGEON, which was much harder to break than TUNNY and was not read, while very confident of TUNNY which was read in great volume. Hence their attitude toward the security of a machine seems based much more on knowledge that it had been captured or had been read, than upon any skillful cryptanalytic assessment. Some cryptographic improvements were made to TUNNY, i.e., SZ-40 was replaced in 1943 by SZ-42.[176] But the Germans did allow the operators to choose settings, and this gave many depths which were read by a small group at GCCS—producing 1.4 million letters of decrypts in May 1943, by a staff of about 20.[177]

The TUNNY machine was produced in considerable quantity—over 1500—and used on landlines all over German-controlled territory, as well as on radio links.[178] No copy of TUNNY was captured until after VE day.[179] Another evidence of German sensitivity to capture occurred in November 1942 when the British captured Army ENIGMA keys in North Africa and the Germans then ceased to send routine messages forming cribs, which set back British SIGINT for some time.[180]

The "Fish" problem was exploited only at GCCS.[181] Even when the U.S. developed some special "Fish" exploitation equipment, it was sent to GCCS and used there.[182] By contrast, ENIGMA was exploited on both sides of the Atlantic.[183] The total number of people involved in "Fish" exploitation was less than 1000, including 600 intercept operators.[184] All the rest were at GCCS and the number of cryptanalysts, who knew what was being read, was under 50.[185] In a good month some 15,000 long transmissions would be intercepted, of which about 2000 were converted from undulator tape and sent to GCCS. Half of these were sent through machine processing to develop statistics, and finally about 500 transmissions were actually decrypted, giving about 2 million characters of clear text.[186] Late in the war, volumes of almost 10 million letters of clear text were produced in a

month, and more could have been produced.[187] Because the clear text did not use the compact telegraphese of the ENIGMA messages, it was much easier to read for picking out intelligence items. The decrypts were produced about a week after the intercepts, so that the "Fish" material rarely produced tactical intelligence, but it produced valuable strategic intelligence to supplement ENIGMA results.[188] Since tactical operations were not usually based on "Fish" decrypts, they could not compromise the TUNNY exploitation in the fashion that the uncovered use of the extremely current ENIGMA messages threatened to compromise that source. Where "Fish" decrypts were reported in Special Intelligence, the source was not identified, and a consumer could easily suppose that *all* Special Intelligence came from ENIGMA. It had proved necessary to *tell* users, especially the Commands, that ENIGMA—not agents—was the source of Special Intelligence, in order to get them to use it and trust it, but there was no need to mention "Fish." Hence security would automatically be better because the users did not know the source, and probably fewer than 100 people, all at GCCS, knew what was actually coming out of the "Fish" traffic.

"Fish" decrypts were used as cribs to break into medium-grade systems (raster), and the "Fish" success was known to the leading cryptanalysts and senior SIGINT administrators on both sides of the Atlantic.[189] But it was probably unknown to almost all high level people in and out of G-2 and the commands, because the exploitation followed the May 1943 agreement between GCCS and the War Department covering ULTRA material—by which time ENIGMA success was fairly widely known.[190] Since the "Fish" success did *not* leak, it appears that the security of Allied cryptanalytic organizations was not compromised. This in turn suggests that the ENIGMA leaks, which reinforced the Fall WICHER evidence and caused the cipher crisis in Germany (in all systems except TUNNY), must have occurred outside the well-informed cryptanalytic circles, possibly from among the thousands of lower-level SIGINT people who knew something about ENIGMA, or from consumers or senior government or military people who were told about ENIGMA but not about TUNNY. It is worth noting that the Russians apparently knew about the ENIGMA success in 1942; at least they asked GCCS for details on the ULTRA success, and the Germans might have captured some Russians who knew too much.[191] Other parties who knew about ENIGMA success included the French, and M.I.6 and OSS, some of whose personnel worked in occupied territory, and were captured.[192]

On the German side, the cipher teleprinters were novel and attractive to use, and since the Germans had no specific reason to doubt TUNNY security, it was never subjected to the desperate security

improvements that ENIGMA experienced. The Germans knew that the French and the Russians were tapping their landline communications, and probably determined that the use of TUNNY thwarted those rear area agents, as a result of capturing some.[193] Because the "Fish" cipher teleprinters were introduced 15 years after ENIGMA came into service, there was no trail of evidence to stain their reputations.[194] Curiously, the Germans never considered betrayal of TUNNY keys, even though they were very concerned with betrayal on other systems.

The security lesson would appear to be that in SIGINT, where the user's confidence in a system is a priceless asset, any decrypts should always be attributed to a target system which is known to be unsolvable, so that if a leak occurs, the target cryptographers will concentrate their security improvements and changes on the wrong system.