For Friedman, File

(material still in

Boxes

Abstracts from: "German Naval Communications Intelligence"
Volume IF-210 - Copy #3
Chapter IV, pp 135-161

WARTIME ACHIEVEMENT ON MAJOR BRITISH SYSTEMS

One of the most striking and significant facts about the German naval communications intelligence organization was its emphasis on low-level codes. An enormous amount of time and energy was devoted to them throughout the war, and usually paid for itself in terms of current reading, -if not in terms of intelligence value. High-grade machine systems, at the other extreme, were largely neglected, or tackled with faint hope and correspondingly sparse rewards. The most uncertain but also the most dramatic results were obtained in the middle ground - that of major British non-machine systems.

If the average of success on the minor codes is represented graphically by a more or less level line, success on these major systems will appear in the form of a wavering curve - climbing to a peak in 1940, sinking in '41, reaching a high peak again in '42, dwindling through early '43, and dropping out of sight in June of that year. The temporary sags and final downward plunge are directly traceable to improvements in cipher security introduced by the British.

As we have already indicated, available sources permit a thorough study only of the British decryption unit, under Tranov. A glance at Chart C at the end of Chapter II will show that the maximum of war-time effort was concentrated here. The most important systems handled by the section were Naval Code #2 (German cover-name Munchen), Naval Cipher #4 (Koeln), and the combined Anglo-U.S. convoy cipher (Combined Cipher #3; Frankfurt).

Success on these systems seems to be connected in a startlingly direct way with German operational successes. For this reason it seems worthwhile to attempt a brief narrative history of war-time achievement on them. Important cryptanalytical developments will be discussed as they occur, but the primary aim is to give a rapid general view of the triumphs and failures involved. (For a list of British systems handled during the war, see Appendix B at the end of this Chapter.)

The Outbreak of War

At midnight on 26 August 1939, five days before German troops invaded Poland, the British introduced far-reaching

COPY REF ID:A66767 TOP SECRET

(43)

changes in their naval codes. Eight of these were being handled by Tranov's section at the time. (44) The volume of traffic in the two most important-Code 2 and Cipher 4 - was small before the war. An average of 15 messages per day was received in the former, and only 15 to 20 percent of the material could be read. (45) No comparable figures are available for Cipher 4, but the percentage was probably lower.

As soon as war broke out, the volume of traffic in all systems increased enormously. The section was temporarily snowed under, not only by sheer quantity of material but also because the new recipherment introduced on 26 August had to be solved. All work on Cipher 4 was temporarily abandoned. (43) Code 2, however, was being read 35 percent by October 1939. It contained a certain amount of information on the war-time organization of the British Navy and the disposition of the Fleet. The effects of the torpedoing of the "Royal Oak" in Scapa Flow and of German battleship activity in the Channel area could be followed in the Traffic. Some data was also obtained on British convoy service.

But Code 2 dealt primarily with patrol vessels. The cipher was the chief source of information on heavy forces. Work on this system was taken up again as soon as more personnel were available, and the traffic was read with some success in November. (45) There had been a 100 percent increase in volume. The daily Admiralty submarine surveys were followed, as well as details of British fleet disposition and cooperation with French naval forces.

It was clear by January of 1940 that the Cipher had far outstripped the Code in importance. In March reading this traffic permitted the Germans to score a major coup, in what was probably decryption's greatest single strategic contribution to the war: "Operation Stratford".

Norway: "Operation Stratford"

In mid-March, 1940, Cipher 4 traffic revealed plans for an Anglo-French expedition against Norway, under the cover-name "Stratford". (46) (For translation of pertinent passages, see Appendix D at the end of the Chapter.) The Germans seized the initiative and invaded Norway on 9 April; the juggernaut was in motion.

2

TOP SECRET

The Cipher was read currently during the campaign. Exact data on British counter-measures, such as landing fields and the arrival of transports at Harstad, were known of in advance, permitting the Germans to take appropriate action.

When Norway surrendered early in June, the decryption unit received a windfall of captured documents.(47) The Norwegians had been equipped with Code 2 code books, as well as several other types, which now became available for study in Berlin. Apparently no Cipher 4 data were captured, but the new store of material was fully exploited as an aid to reading this cipher.

The Norwegian episode was a banner period for Tranow's section. He was forced to rest on these laurels for some time. By August new decryption problems had arisen which accumulated steadily during the following year.

The British Improve Their Cipher Methods

A general cipher change took place in Cipher 4 and Code 2 on 20 August 1940.(48) The latter, formerly a 5-place number code, now became 4-place, similar to the Cipher. Both systems were equipped with 5-place indicators. One hundred thousand of these were divided between them, in a manner unknown to the Germans, so that externally the two systems were indistinguishable. At the same time separate Cipher 4 keys were introduced for the following areas: 1) North Sea and North Atlantic; 2) Mediterranean, East Indies, and South Atlantic; 3) East Asia, Australia, and New Zealand. There were also separate keys within these areas for different traffic circuits.(49)

In October the Code was subdivided into 2 systems, one to be used chiefly for patrol vessels, minesweepers and local convoys, the other for personnel traffic and independents in the South Atlantic and Indian Ocean. An innovation was introduced in the latter; special reciphering on the one hand for the address - on the other hand for the text.(50)

Thus in the latter half of 1940 the task of Tranow's section became increasingly complex and bewildering. The Code was neglected in favor of the Cipher, where success was meagre.

Then, on 20 January 1941, a serious crisis arose. The British introduced enciphered indicator groups for Cipher 4 and Code 2 and all German decipherment of these systems stopped instantly.(51) Headquarters was deeply shaken. Teubner, then head of communications intelligence, ordered that a directive

be sent to all groups and flotillas warning them that no information on the positions and movements of British surface forces could be expected for some time, owing to a "basic" cipher change -- as yet unfathomed.

Intensive research was begun on the new problem. The nature of the change was soon determined, but the amount of actual reading done remained negligible throughout the summer. As was usual in such periods, the less important and less secure systems were heavily exploited.

On 1 September 1941 the general indicator group book for the Cipher and the Code changed; it became extremely difficult to discriminate between the systems.(52) Four-place non-enciphered indicator groups had been introduced. This would have made reading easier -- once the traffic was differentiated, if the Germans had had time to take advantage of it. But in two months the indicator book changed again, and the whole procedure of discrimination had to be repeated.(53) Occasional currency in reading the systems was achieved in the interim, however, and again in December 1941. Scattered information was gleaned on convoy and mership routines, the maneuvers of heavy units were followed sporadically, and Admiralty's daily surveys of German submarine positions were read.

On the 1st of January, 1942, these sources were cut off temporarily. The British issued new code books for both systems, and introduced numerous one-time cyphers for special areas.(54) Reconstructing the code books was only a matter of time, but the one-time cyphers were, as Tranow puts it, "invulnerable". The starting(55) point and recipherment for individual messages were used only once -- never repeated. Increased use of this "absolutely secure" method hampered decryption throughout the year.(56)

The Cipher, especially, was affected. In addition to the one-time pads, increasingly frequent recipherment changes were introduced. Half-hearted attempts to apply IBM techniques were made and failed; reading was no longer possible.(57) (58) Morale problems became acute during the summer and fall, and by December most of the Cipher 4 personnel had been transferred to other work.(59) A chapter which began with "Operation Stratford" had closed.

In another respect, however, 1942 was a year of signal triumph for German communications intelligence. The combined

~~TOP SECRET ULTRA~~ COPY ~~TOP SECRET~~

Anglo-U.S. convoy cipher was broken, read with a high average of success, and its intelligence acted upon by the German submarine fleet.

Combined Cipher No. 3: A Triumph for German CI

The Combined Cipher for Atlantic convoys was introduced in October 1941, before the United States entered the war. On 24 January 1942 a special subsection took over work on this traffic.[60] It was read about 100 percent during February and March, 80 percent from June to mid-December and again with some success from February to June 1943, when it was replaced.[61] During this entire period Allied shipping losses in the Atlantic by U-boat action averaged 360,000 tons monthly; after June 1945 the average dropped to 60,000. Undoubtedly other factors were involved, but the inference seems clear; decryption had made a vital contribution to the war. (See the Chart at the end of this Chapter.)

The first gap in the long history of success on the Combined Cipher came in April and May 1942. On 1 April indicator groups for all 4-place number systems changed, and the two 5-place groups which formerly had distinguished Combined Cipher messages disappeared.[62] An enormous amount of work was required to handle this mass of externally similar material. A general recipherment change on 1 May and indicator group change on 1 June added further complications.[63]

But the decryption unit had better luck than it had expected. The summer and fall was a peak period. Extensive use was made of IBM cards, especially after the introduction in August of separate reciphering for the address and text.[64] This had already taken place in Code 2 and Cipher 4. No serious difficulties were involved here, as long as the keys remained in force for a month. Later in the year they began to change semimonthly and reading slowed down.

The second major breakdown in German success with the Combined Cipher came in December 1942. On the 15th of that month the British reintroduced enciphered indicator groups for the three main systems.[65] Code 2 and Cipher 4 were being read almost currently prior to the change. Now a severe drop occurred. The U-boat war was affected; Cominch demanded swifter and better results from decryption.[66] An upheaval took place in the British section. New working methods were formulated and

5

introduced.[67]   The Combined Cipher staff was doubled by the addition of former Cipher 4 personnel. Nevertheless it was clear, Tranov remarks, "that under existing circumstances the former peak of decryption success would never recur."[68] It was estimated, that henceforth current reading would be impossible until at least six months after a code book change.

As we have indicated, some reading was achieved on the Combined Cipher in the spring of 1943. This was due in part to the fact that the code book remained in force longer than usual. On 1 March the Code 2 book changed, but the Combined Cipher continued as before. Tranov found this "astounding".[69] He hazarded two reasons for what seemed to him gross negligence on the part of the British: 1) the Combined Cipher, though certainly more important than either Code 2 or Cipher 4, was used less extensively, and 2) out of about 2500 4-part number messages per day, it would be extremely difficult to separate the 150 - 180 messages sent in the Combined Cipher. Actually this feat was accomplished by IBM techniques, and the U-boat could again be supplied with data on convoy movements in the Halifax and Gibraltar areas.[70]   The Combined Cipher was withdrawn on 10 June 1943, and replaced by Naval Cipher #5. This new combined system was never read by the Germans.[71] Their period of triumph ended abruptly.

The Decline

From June 1943 until Germany's surrender in May 1945, the story of the British decryption unit is one of frustration and failure. The wheels continued to revolve, chiefly on their own momentum, but the production line was almost bare.

The two final and conclusive improvements in the main British systems occurred in December 1943 and January 1944. One was the introduction of a stencil subtractor making possible a daily change of key (on 1/12/43 for Code 2 and 1/1/44 for Cipher 5). The other was the adoption in January 44 of a regular six month code book change. Formerly the recipherment keys had changed every 7, 10 or 15 days, and the code books every 14 to 18 months.

The whole status of decryption was altered as a result of these developments. Tranov summed it up as follows: "Reading the systems for operational value will no longer be possible, except in cases where the current code book is captured."[71] In that event, solution of the daily key would be possible

Tranov managed to retain a staff to meet the possible contingency, though some voices were raised in protest. Germany's military situation was desperate. The possibility of capturing enemy documents became more and more remote, and it seemed unlikely that decryption would ever again make any vital contribution to the war. This pessimism was fully justified by the event.

At the end of 1943 or early in 1944 (the exact date is uncertain), and exhortation to all naval RI personnel appeared, [72] which seems implicitly to accept the failure of cryptanalysis. It suggests an alternative: the development of traffic analysis. This branch of communications had been neglected to a certain degree in favor of cryptanalysis. A higher standard of performance was now required. Traffic analysis, it is stated here, could not equal decryption in military value, but since the latter's task had become so difficult, the former would be forced to assume greater burdens.

A general report on the status of naval cryptanalysis, written in March 1945, contains the following succinct statement:

> "The main enemy systems - British, American and Russian - have been so much improved within the last two years that their recipherments are either completely secure or can be solved only with an enormous number of personnel and a maximum amount of difficulty."[73]

Actually, currently readable traffic was by then limited almost exclusively to British coastal and tactical systems, and the Merchant Navy Code.

The statement quoted above expresses a fact. It also implies an attitude. There could be no question of recovering lost ground; the game was up. This tone had become increasingly apparent in the decryption reports of the two preceding years. It gave the occasional pep talks and assurances of final success a peculiarly hollow ring.

A NOTE ON AMERICAN SYSTEMS

The main intention of the preceding pages was to exploit available sources for the story of German achievement on major Allied systems. As a result of this emphasis we have neglected those areas of activity which were scantily documented or which led to meagre success. German attacks on American systems fall into one or both of these categories. However, a word should be said on the subject.

All combined ciphers were handled by the British section; hence German study of the Combined Cipher Machine (CCM) may be followed in the decryption reports. In April 1944 the appearance of a new type of machine traffic was noted. It was described as five-place letter traffic with a pronounceable indicator.[74] During the investigation which proceeded throughout the summer, a table of these initial indicators was compiled to facilitate recognizing the traffic.[75] In October seven messages with identical first and second indicator groups were discovered; it was deduced that the system involved non-reciprocal substitution alphabets and was based on plain text.[76] Research on the CCM ceased on 31 January 1945.

The Navy Hagelin and the strip-cipher DUPYH were handled in the American section. We have no decryption reports from this section; according to Schulze, who headed it from January or February 1944, all records were destroyed before the surrender.[78] Our only source of information is the testimony of various P/W's which is in many instances conflicting and obscure. Apparently no more than two or three days of traffic in the Navy Hagelin system were read, though one I-report states that it was solved except for a method of determining the true settings, which was subsequently learned from the Army.[79]

The Japanese Navy at one time gave a set of DUPYH strips and settings to the Germans, enabling them to read the traffic until the keys went out of force. It is stated that no real intelligence was gained,[80] but the Germans were thus given an insight into strip methods. Nevertheless, no other strip systems were solved.[81]

Kapt. Otto von Baumbach, chief of the Naval Intelligence office, and in general a great admirer of the work of RI, stated that no information of any value was gleaned from the study of American naval systems.[82]

CONCLUSION

We have discussed German pre-war and war-time decryption activity in so far as we know it chiefly in terms of outward achievements. In order to assess the reasons for those achievements, and for the failures which accompanied and finally outweighed them, we must look for a moment into the inner workings of the organization.

Thoroughness, efficiency, technical skill and ingenuity were all present in a very high degree. These factors encouraged the development of specialization, of carefully formulated and executed patterns of work. When applied exclusively to low-level systems, as in the pre-war years, they brought almost certain rewards. But when these familiar methods were carried on into the war some of their inherent weaknesses gradually became apparent.

During the first few years of the war, as we have seen, German decryption scored heavily against its primary target-- the main British systems. As these systems became more and more secure, success in reading them diminished. By 1944, the cumulative weight of difficulties had finally crushed all German efforts to overcome them.

The first point to be noted in this connection is the excellence of British cipher security; certainly the Germans faced a formidable obstacle. But there is a further consideration. Because of a long tradition of success with hand methods, the German naval cryptanalysts tended to regard them as the ultimate decryption process. Encipherments which were beyond the range of hand methods -- such as the one-time pad and machine systems -- they were apt to consider unbreakable. (Their faith in the security of the Enigma is a case in point.)

As a result of this conservatism, the naval decryption section was slow to grasp the vital importance of machine techniques. The development of the Hollerith section (discussed above under 'Administration') illustrates the lag between "discussion" and actual execution of a new idea. The conviction and drive necessary to cut through tradition were lacking; innovations were introduced only after crucial time had been lost, and often depended entirely on fortuitious circumstance.

REF ID:A66767

Coupled with this caution in taking up new methods was an insistence on current production. This could usually be achieved with the low-grade systems by routine procedures, but the development of a radically new technique for the more secure systems might have meant a long period of suspension before any results were arrived at -- or ultimate failure. It would be a gamble -- an enterprise which the naval cryptanlysts were apparently loath to undertake.

With all its professional efficiency, the German naval decryption organization seems indeed to have suffered from a basic dry rot of conservatism and inflexibility.

READING ENEMY TRAFFIC

APPENDIX A

Notes on Personnel Requirements

In March or April 1941 a total of 64 men were assigned to the Naval Cipher, on a 4-watch basis. Four more were needed per watch. A total of 40 men were assigned to one of the subdivisions of the Naval Code, and 8 more were needed. The other subdivision of the Code had 7 men, working only by day. Six more men were needed to build up a 2-watch schedule. The total complement[83] desired for the main British systems alone was thus 165 men.

In March 1945 naval decryption total personnel requirements were stated as follows: for current readable traffic of all countries - 155, for research on main British systems - 85, thus a total of 240.[84]

From January 1944 to January 1945, the staff of the Naval Code subsection dropped from 198 to 94.[85]

Tranov states that he was employing about 150 men at the end of 1940. By December 1942 his staff had increased to about 275. He wanted to double the number, but did not succeed in doing so. In February 1945, he remarks bitterly, the total number of personnel in the entire cryptanalysis section was 275.[86]

COPY

REF ID:A66767

READING ENEMY TRAFFIC

APPENDIX B

LIST OF BRITISH AND COMBINED SYSTEMS

HANDLED DURING THE WAR

The following information was taken from T-517 through T-520, passim, and from I-12 and I-93.

System	German Covername	Remarks
Naval Cipher No. 4	Koeln	First read mid-October 1939. Peak reached in 1940. Increasing difficulties after January 1942. No longer read after mid-1943.
Naval Code No. 2	(braun and blau) Muenchen	Read with considerable success, from start of war to December 1943, but with frequent gaps. Not read after January 1944.
Combined Cipher No. 3	Frankfurt	Introduced October 1941. Read about 80% from February 1942 until 15 December 1942. Difficulties, then success in April and May. System replaced in June 1943.
Interdepartmental Cipher	Bremen	Work begun mid-1940. Read sometimes up to 100%. In force until end of 1942.
Interservice Code	Danzig	Apparently replaced interdepartmental Cipher in July 1942. Not being read by November 1942.

12

System	German Covername	Remarks
Naval Shore Code	Stettin	Worked on with little success in 1941-1942. Volume of traffic small.
Fleet Code	Hamburg	Worked on throughout the war. Very little traffic -- few results. Attempt to read North African landing traffic with captured code-book unsuccessful, owing to extensive use of covernames in text.
Mersigs	Gallien	Work begun spring 1942. Read currently from start of 1944 to end, except when one-time pads were used.
Bentley's Phrase Code	Tatra	Worked on in 1943. Work stopped in May 1944, after introduction of one-time pad traffic.
Government Telegraph Code	Alpen	Read with some success in 1940. Most of traffic transferred to Naval Shore Code in 1941. Work stopped during 1944.
Auxiliary Code		Worked on at start of war. Pinch of code-book in October 1940 led to current reading.
Delivery Groups		Worked on from start of war. Often useful for reading other systems, and for traffic analysis. Read currently at times in 1942 and 1943. Not read after February 1944.

System	German Covername	Remarks
Nyko Syko	Taunus Rhoen, also Taunus	Worked on in 1943. Volume usually too small for current reading. Work stopped in 1944.
(Torpedo A/C Code)	Spessart	Work stopped July 1944 -- volume too small.

Small Ships
  Basic Code
    Cofox)
    Medox)
   Foxo
   Loxo
 	
   Traxo
	Hunsrueck
	
	Eifel
	(Loxo also called Deister in Medit. area)
	
	Suentel
		Most of this traffic read currently in late 1943 and throughout 1944.

Ecco	Harz	Coastal convoys, chiefly in Liverpool area. Out of force September 1943. Apparently read up to this time.
Bridford Code	Ruegen	Pinched from British speedboat in November 1943. Traffic between Admiralty and two steamers in Sweden, also battleship flottila. Copies sent to outstations for immediate reading.
	(Fq 003)	Used between "Shipminder" and "Shipminder London". Apparently read.
	(Pq 008)	Interallied. Used in landing and supply operations. Difficult to read because of many covernames and abbreviations within text.

System	German Covername	Remarks
Combined Assault Code	Tauern, also Altona	Used in North African and Normandy landings. Special systems for Atlantic and Mediterranean invasion coasts. Traffic in former partly read in fall 1944.
Combined D/F Reporting system	Stralsund/Kolberg	First appeared August 1944. Reasons give: 1) lack of personnel, 2) traffic not operational.
Combined Cipher Machine	Ulm	Worked on from May 1944 to January 1945. Not broken.

READING ENEMY TRAFFIC

APPENDIX C

Berlin, 20/1/1937   Part of A III b 2128/36 Top Secret

1) To: Abwehr III f West

   Subject: British number messages

   Reference: Abwehr 1579/36 Top Secret III f West of
                2/10/1936

1) The British number messages which you sent could not
be deciphered, since they also lacked all the characteris-
tics essential for decryption (such as call signs, origi-
nating stations, receiving stations, time/date groups,
frequency data, dates, etc.) Moreover the amount of traf-
fic is not sufficient to permit a break by means of sta-
tistical data.

2) Again we wish to emphasize the fact that as far as
Italy is concerned, the German Navy disclaims all interest
in British Naval traffic owing to the suspension of intel-
ligence activities (B-Dienst) against England. Therefore
the Italians are under no circumstances to be allowed to
form a different impression. For this reason it is requested
that the Italians be informed that they should no longer
relay any British traffic to us since it will not be de-
ciphered here.

Besides we have no interest at this time in British traf-
fic.

2) File under A III b Top Secret 5-1

                                    Signature (39)

TOP SECRET

READING ENEMY TRAFFIC

APPENDIX D

"OPERATION STRATFORD"

(Extract from review of work done on British systems
from 1939 to 1941, written by Tranow).

    ...In mid-March the Anglo-French assault on Norway --
known by the cover-name 'Stratford' -- was learnt of
through Koeln (Naval Cipher #4). Standing readiness 48
was ordered for the troops and 95 for the convoys...

    ...As soon as the (German) attack on Norway began..
it was possible to read currently of almost all the
British...countermeasures. The proposed landing fields
... were known. The arrival of transports at Harstad
was determined exactly to the hour, and so far in advance
that our own (i.e. German) forces were able to attack
them.

    The strategy of cooperation of the French and
British surface forces and their combined action in this
campaign were also revealed through Koeln. Even the of-
ficers in command were determined by means of this traf-
fic.(87)

REF ID:A66767

READING ENEMY TRAFFIC

References

(1)   I-12, p. 13
(2)   T-514, 22 March 1935
(3)   T-514
(4)   T-515, 23 March 1940
(5)   T-514, 5 September 1936
        T-516, 4 October 1941
(6)   T-517, 7 August 1941
(7)   T-517, 22 May 1942 and 4 March 1943
(8)   T-517, 6 March 1943
(9)   I-146
(10)   I-12, p. 3
(11)   T-519, 9 December 1943 and 10 December 1943
        I-12, p. 5
(12)   CSDIC/CMF/Y37
(13)   T-519, 10 December 1943
(14)   I-143, p. 7
(15)   T-519, 1 August 1944
(16)   T-519, 1 June 1944
(17)   T-517, 2 December 1942
(18)   T-520, 8 January 1945
(19)   I-12, p. 5
(20)   T-517, 3 September 1942
(21)   T-519, November 1944
(22)   T-514, 23 September 1937
(23)   T-514, 6 January 1937
(24)   I-12, pp. 13, 14, 15
(25)   I-93, p. 10
(26)   T-519
(27)   T-514, 6 May 1935
(28)   T-515, 8 March 1940
(29)   T-514, 22 March 1935
(30)   T-514, 27 May 1933
(31)   T-541, 25 August 1937
(32)   T-514, 7 June 1937
(33)   T-514, 5 June 1937
(34)   T-515, 18 July 1939
(35)   T-514, 30 May 1935
(36)   T-514, 22 March, 30 May, and 12 November 1935

TOP SECRET ULTRA COPY   TOP SECRET

(37)	T-514, 9 September 1935
(38)	T-514, 9 July 1935
(39)	Tranov's Report on British System with 4-place recipherment, 13 April 1939.
	Originally a part of T-517; filed in its chronological position in T-515 by OP-20-G.
(40)	T-514, 2 January 1937
(41)	T-514, 6 January 1937
(42)	T-514, 23 September 1937
(43)	T-517, 13 October 1941, p. 3
(44)	T-517, 13 October 1941, p. 1
(45)	T-517, 13 October 1941, p. 4
(46)	T-517, 13 October 1941, p. 7
(47)	T-517, 13 October 1941, p. 8
(48)	T-517, 13 October 1941, p. 11
(49)	T-517, 13 October, 1941, p. 12
(50)	T-517, 13 October 1941, p. 14
(51)	T-516, 23 January 1941
(52)	T-516, 19 September 1941
(53)	T-517, 11 November 1941
(54)	T-517, 21 December 1942
(55)	T-519, 31 May 1944
(56)	T-519, 2 October 1942
(57)	T-517, 3 July 1942
(58)	T-517, 3 September 1942
(59)	T-517, 8 January 1943
(60)	T-517, 6 February 1942
(61)	I-12
(62)	T-517, 4 April 1942
(63)	T-517, 12 May and 5 June 1942
(64)	T-517, 20 August 1942
(65)	T-517, 16 December 1942
(66)	T-519, 1 June 1944
(67)	T-517, 8 January 1943
(68)	T-519, 1 June 1944
(69)	T-517, 19 March 1943
(70)	T-517, 19 March and 2 April 1943
(71)	T-519, 1 June 1944
(72)	T-519, (date uncertain, late 1943 or early 1944)
(73)	T-520, March 1945
(74)	T-519, 18 May 1944
(75)	T-519, 16 June 1944
(76)	T-519, 5 October 1944
	T-520, 9 January 1945
(77)	T-520, 10 March 1945
(78)	I-141, p. 2
(79)	I-6, I-144
(80)	I-93, pp. 8, 9;
	I-6, pp. 15, 16
(81)	I-147, p. 25
(82)	I-165

TOP SECRET

(83)   T-516, (undated, March or April 1941)
(84)   T-520, March 1945
(85)   T-520, 9 January 1943
(86)   I-12, p. 5
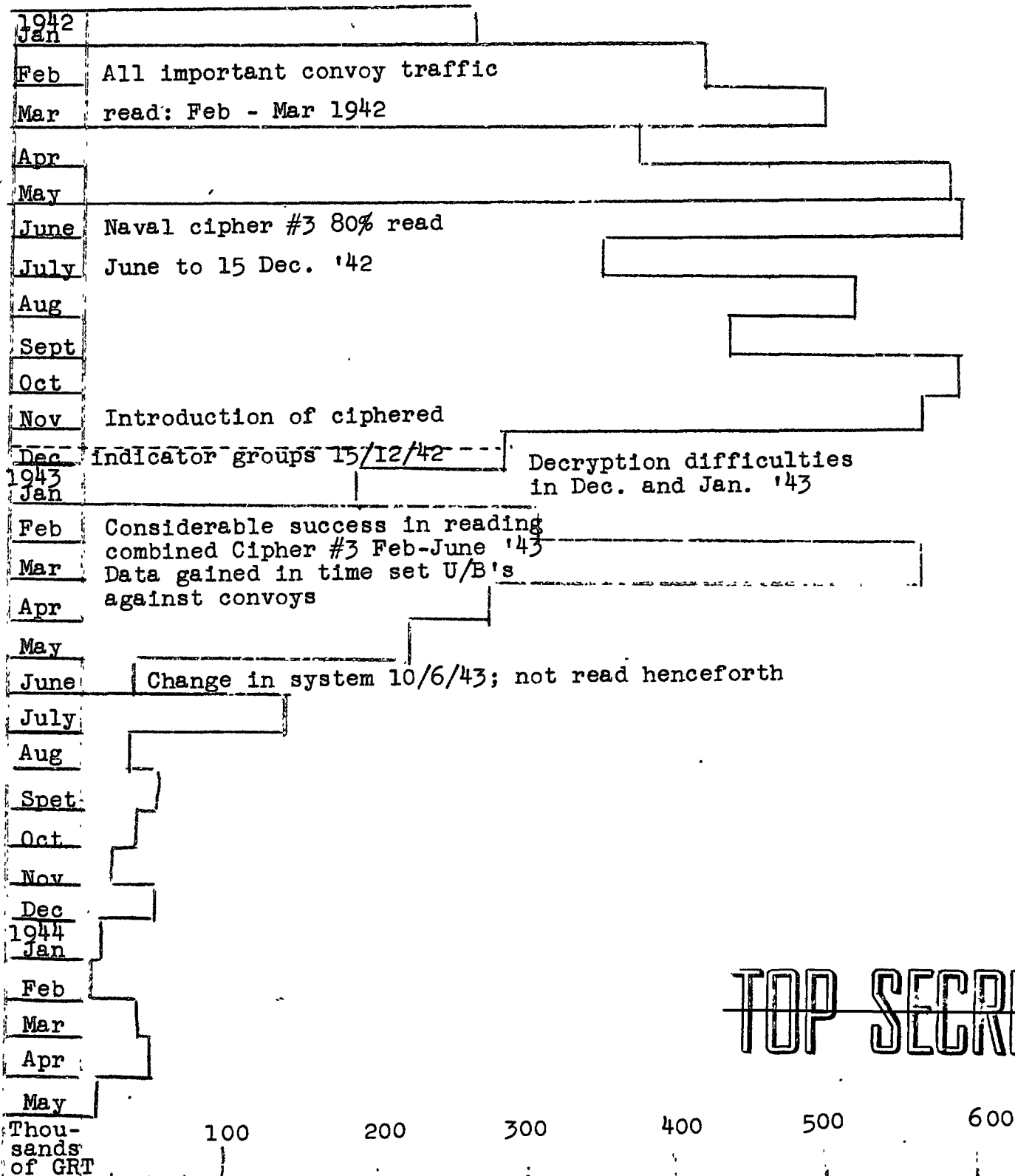(87)   T-517, 13 October 1941, pp. 7, 8, 9

COPY

1942 Jan	
Feb	All important convoy traffic
Mar	read: Feb - Mar 1942
Apr	
May	
June	Naval cipher #3 80% read
July	June to 15 Dec. '42
Aug	
Sept	
Oct	
Nov	Introduction of ciphered
Dec	indicator groups 15/12/42
1943 Jan	Decryption difficulties in Dec. and Jan. '43
Feb	Considerable success in reading
Mar	combined Cipher #3 Feb-June '43 Data gained in time set U/B's
Apr	against convoys
May	
June	Change in system 10/6/43; not read henceforth
July	
Aug	
Spet	
Oct	
Nov	
Dec	
1944 Jan	
Feb	
Mar	
Apr	
May	

Thousands of GRT   100   200   300   400   500   600