[WILLIAM F. FRIEDMAN - TRIP TO ENGLAND, 1943]

~~SECRET~~

RANDOM NOTES

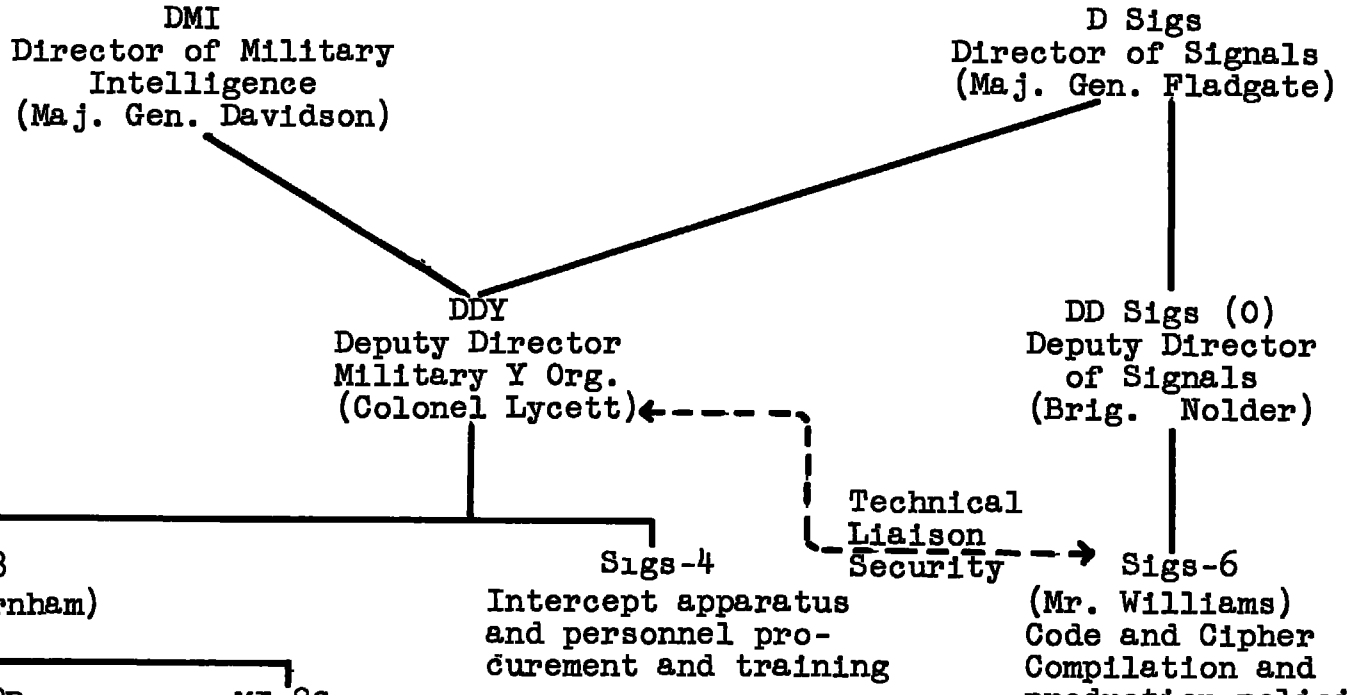
While en route to visit the War Office intercept station at Beaumanor I undertook to obtain a bit of information from Colonel Lycett regarding the organization and functions of the War Office bureau in which he was assigned and the following notes are based upon the answer to various questions I raised.

Colonel Lycett drew a rough chart showing where he fitted in the organization and this is attached hereto. The duality in responsibility to two different branches of the War Office organization is interesting to note in the case of Colonel Lycett's position inasmuch as he is responsible to both DMI and the Director of Signals. Another interesting thing to note is that although the military wing which comprises No. IV and No. VI Intelligence Schools of GC & CS belonged to MI-8A, Colonel Tiltman, the commander of the military wing reports directly to Colonel Lycett and not to the Chief of MI-8, Colonel Vernham. It is also interesting to note that Brigadier Nolder is responsible for the production and distribution of code and ciphers but these are printed at Oxford by a group which is under GC & CS.

Signals 4 is responsible for the procurement of Y personnel and equipment for them as well as for training. When the unit is completely trained it is turned over to Home Forces or to Overseas Commands.

On the staff of superior units of Home Forces and Overseas Forces is an officer called GSIS representing General Staff Intelligence and Signals. This officer is familar with the functions and work of the GC & CS and therefore does not allow his unit to undertake Y work inconsistent with higher policy although Y work in these forces is theoretically independent. Signals VI has practical control by virtue of its control over the personnel and equipment supplied them. Home Forces interception is autonomous but usually there are a few sets assigned to high-grade intercept work at Harpenden which is the Home Forces Y Group Headquarters station.

~~SECRET~~



*Military Wing of GC & CS (Col. Tiltman) including No. IV and No. VI Intelligence Schools come under MI-8A but Col. Tiltman reports directly to Col. Lycett and not to Col. Vernham.

The headquarters of a field force has a Y group force composed of two separate parts. First a special traffic analysis group and second a radio intelligence group. Each army has an "A" type section which consists of a special radio section type "A" and a traffic analysis section type "A".

Each corps normally has a "B" type radio intercept and a "B" type traffic analysis unit.

To handle the work and output of these units there is at the headquarters of field forces a GSO-1 who is the GSIS of the unit and has a staff with much the same duties as MI-8 of the War Office. The GSO-1 is usually a Lieutenant Colonel.

At Army there is a GSO-2 who is a Major and is the GSIS officer. He devotes his entire time to Y work.

At Corps there is no special Y officer but one of the three intelligence officers on the staff maintains liaison with the intelligence staff and gets from them any identifications available which identifications he fuses with intelligence he is able to obtain.

At Division there is no Y officer specially assigned.

A type "A" radio intelligence unit has twelve receivers and three direction-finding sets. The traffic analysis group consists of ten officers and twenty-six other ranks.

The type "B" radio intelligence unit has eight receivers and one direction finder. The traffic analysis consists of three officers and twenty other ranks.

As an example of the kind of work done by a type "A" unit the messages of the Phoenix cryptonet was cited. This was obtained by a type "A" unit of the Montgomery Army and was first noted in the Middle East from what was sent to GC & CS where it was found that solution could be obtained. Whereupon BP supplied them with Typex equipment and sent them solved keys so that the unit in the field could decipher intercepted messages locally; this was done with the greatest secrecy. All the traffic thus handled by the type "A" unit was, however, sent to BP. Colonel Lycett indicated that on account of the danger and the necessity for speedy communications which are difficult to have in the field this experiment will never be repeated and it has been decided as a matter

of policy to keep all of this high-grade material under very close control of GC & CS at BP.

Colonel Lycett mentioned a "Wireless Telegraphy Board" which was set up after the last war and corresponds to our Joint Communication Board at Washington in certain respects. The chairman of the board is a Lieutenant Colonel or an officer equivalent in rank in the other services. The members of the board are the directors of signals in the three services. The chairman is in turn an Army, Navy, or Air Force officer who gets a four-year detail in the job. The duties of the board are mainly to coordinate all matters affecting communications of the three services. The name of the board is misleading since it deals with all types of communications, radio, cable, telephone, etc. The name has stuck because it started off as a frequency allocation board for the three services. In peace the Postmaster General has control over this matter of allocation but in wartime this board takes charge.

~~SECRET~~

SIGNALS--6 AT THE WAR OFFICE

(Visited on June 10)

A small central organization called Signals-6 (with three subsections) is maintained at the War Office for work in connection with (a) the compilation and distribution of War Office and British Army codes and ciphers, (b) the development, construction, and distribution of cipher devices, and (c) the security of military cryptographic communications. The group is headed by Mr. J. H. Williams, a Civil Servant who has been in charge of these activities for many years. He has a staff of four officers and about four or five clerks.

As regards code and cipher compilation duties, the work done here is largely executive or administrative in character. Plans for new editions of codes are made, distribution tables and data compiled, records of holders maintained, etc. No actual compilation or printing work is done here, as these functions are performed at Oxford by the inter-service code and cipher compilation and reproduction agency under Commander R. E. Hok.

With regard to security studies in connection with their own traffic, the only thing done is to keep detailed records of traffic volumes in the various systems. All outlying headquarters notify the War Office, by telegraph or radio, of the total monthly traffic counts (number of groups) or outgoing cryptographic communications, except as regards messages to the War Office. The in and out traffic of the War Office is counted in this section from records made available to it by the two signal centers maintained at the War Office (see below). Attached to each large overseas command is a Force Security Officer who maintains the same general type of record as regards the communications within the force itself and from the force headquarters to other Commands, except London. Monthly summaries of intra and inter-unit traffic counts are sent by the various Force Security Officers to the War Office where they are combined into one large report. Thus these records afford the basis for security control to insure that no system is loaded beyond the safety point.

It is to be noted that the job of Force Security Officer, who has one assistant as a rule, is a specific assignment on the Signals Staff of each command. The policy of having these officers has been established for only about one year but Mr. Williams assured me that the results were most beneficial and that they turned up "an amazing number of things".

The record keeping for the security studies referred to under Par. 3a is done by three women. They draw up, as regards systems using general subtractor tables, "depth charts", or what we would call overlap charts, showing the superimposition of messages in the same segments of the subtractor tables. They also look for stereotypy, study the beginnings and endings of messages, and note the special habits of the code clerks who encode and encipher the messages; in fact, they actually keep records showing the idiosyncrasies of individual clerks so as to have a guide for admonishing them when necessary. Every cryptographic message in and out of the War Office is registered and studied from these points of view. Just how only three women could do this entire job is not clear but I saw the depth charts, the books with the various notations as to habits of code clerks, etc., so that I am sure there was no great amount of exaggeration.

With regard to studies on Typex traffic, somewhat similar data, especially as regards volume, are kept. Incidentally, here is a list of the ten different sets of rotors maintained for Typex communications:

(1) For special communication only between the War Office and the topmost commanders (only the C in C's) of overseas Commands.

(2) For general communication between the War Office and the commanders of all overseas forces and for intercommunication among those commanders.

(3) For intercommunication among field units from GHQ to Corps, inclusive.

(4) For special interservice communication, with a narrow or limited distribution (high commands).

(5) For general interservice communication, with a wide distribution.

~~SECRET~~

For intercommunication among field units from Corps to Divisions or smaller units equipped with Typex machines there are five regional sets of rotors, as follows:

(6) A set for units of the Home Forces (U.K.).

(7) A set for units of the European Theater.

(8) A set for units of the North African Theater.

(9) A set for units of the India Theater.

(10) A set for units of the Southwest Pacific Theater.

Sets of subtractor tables are also allotted, according to the foregoing specific and general types of distribution, for use between the War Office and tactical commands, for use within theaters, and for interservice use.

Mr. Williams and I had a brief discussion regarding the new device called "Slidex", an advance sample of which I had seen in C Branch some time before my trip. He demonstrated a more recent model. (The Slidex is to replace the device called the "Kodex", which has proved to be insecure.) This device is to be employed for radiophone communications in the combat area and will be provided with separate sets of cards for the various services such as Artillery, Quartermaster, Medical, etc. Besides the foregoing there will be a general "operations-signals" card; in addition a "unit card", which will be blank and can be filled in with meanings by the individual unit commanders, will be provided. As regards the "cursors" for the Slidex device, they plan to have one set of cursor keys for army to division, inclusive, and another set for division to battalion, inclusive. The Slidex is a very compact device and is made to fit into the trouser's pocket of the battle-dress uniform. Its cryptographic security is fair. I was advised that several copies of the latest device will be sent to Arlington Hall in about one month.

Mr. Williams showed me a copy of each of their two principal types of code books. There is a large code (W.O.) for communications between the War Office and the headquarters of overseas Commands. This is a 100,000 group, two-part code using five-digit equivalents and the groups are enciphered by means of the usual one-time pads or large general subtractor

tables. There is a smaller (10,000 groups) four figure, two-part code for communications from GHQ down to and including division (Inter-Service Cypher). This is to be used with subtractor tables and, within a short time, with the new "stencil subtractor frame". These codes so far as the larger Commands are concerned are employed as standby systems for the Typex machine; smaller Commands abroad which do not as yet have the Typex, however, rely entirely on the code with either the subtractor tables or the SS frame. For communication within Brigade there is a small two-part code called the "Brigade Cypher" which is enciphered by subtractors and a new, small SS frame has been developed for this purpose.

No cryptanalytic security studies whatsoever are undertaken by Mr. Williams' organization, but when a problem requiring cryptanalytic techniques does arise it is referred to Colonel Tiltman in his capacity as "Chief Cryptographer to the War Office". As a specific example, he was given the task of ascertaining the security value of the "Stencil Subtractor Frame" for general communication purposes (not for synoptic weather reports) and when I was a BP the research group under Major Morgan was just completing a rather detailed study of the security afforded by the device, based upon a large number of test messages which had been prepared for the purpose. Tiltman retained the "answers" and Morgan's group tried to solve the messages by cryptanalysis. The group had made little progress and reported that the cryptographic security is very high.

In connection with the Typex machine and the new plugboard arrangement therefor, I learned that all of these machines of the Mark II type (the present large machine) distributed down to and including Army, are to be provided with a plugboard which is on the reflector or reversing rotor (13 connector wires ending in plugs to be inserted in jacks).

It was in Mr. Williams' section that I first learned about the new Mark VI Typex machine for field use, developed, as was the large Typex, by the RAF. It was described to me and was stated to have an operating speed of 90 characters per minute. When I expressed a desire to see a model, arrangements were at once made with Wing Commander Johnston of the Air Ministry to see one. A report will be found under the next section.

~~SECRET~~

Also under Mr. Williams is the "Central Cipher Office" which is like our War Department code center, but does work only for the following four catagories:

(1) Paymasters.—There are about 20 of these scattered throughout the United Kingdom at the Headquarters of the regimental areas from which the various regiments are recruited.

(2) Record Offices.—About 20 scattered as above. These are equivalent to local regimental Adjutant General's Offices.

(3) The Soldiers and Sailors Family Associations.—These are likewise offices scattered throughout the United Kingdom and deal with the welfare of the troups abroad.

(4) Army Agents.—For officers' pay; likewise scattered throughout the regimental areas in the United Kingdom.

The central cipher office handles between 34,000 and 38,000 code groups per day. It is "manned" entirely by ATS, a total of 38 being employed there as code and cipher clerks. All of them are skilled in the use of the Typex machine and in the handling of code books with subtractor tables. The central cipher office is administered by five ATS officers, the leading one a Captain.

There are eight Typex machines in this office; ten ATS comprise a working shift. Supervising the shift is one duty officer in charge and one assistant duty officer who receives and registers all outgoing and incoming messages for cryptographing, indicates the system to be employed and passes the messages on to the code room for actual handling. The Typex machines are serviced and maintained by about six members of an organization called the REME, standing for the Royal Electrical and Mechanical Engineers. This is a new corps composed of maintenance personnel taken from all services. The purpose of establishing this separate corps was to eliminate the large amount of duplication which had been found in this field. It apparently is working very well.

The training of the ATS code and cipher operators is done at "No. III Intelligence School", which is located at a

secret address in London. Two courses are given there. The first is a course in medium-grade work lasting two weeks, where instruction is given in the handling of codes with subtractor tables and in the use of the Typex. The capacity of this course is 20 men and 10 women per week. This course is to be extended later to three weeks, when the Mark VI Typex comes into use. The second, or high-grade, course is given to individuals who have had the medium-grade course and have returned, after practical experience has been obtained in the work, to do an additional one month's course in more advanced code work. The capacity of this course is 40 men and 30 women per month.

I was informed that there is another much larger code center in the War Office designated as "C-6-Telegrams", but did not visit it. The latter handles all the messages directly to and from the War Office in connection with intelligence, operations, supplies, administration, etc. The entire section handles, on the average, 90,000 code groups per day. This organization is the equivalent of our War Department Code Center and has a large staff with 30 Typex machines, which are also operated by ATS. I was informed that the supervisory personnel of "C-6-Telegrams" are all civil servants, mostly "old-timers". In connection with these supervisory "civil servants" I learned a fact of interest and significance so far as the British are concerned. When I asked Colonel Lycett why this emphasis was placed upon having civil personnel in charge he informed me that under the British system and since the time of Cromwell's descent upon Parliment, the principal heads of sections in the War Office are all civil servants. In particular, the Permanent Under Secretary of State for War is a civil servant who acts as a watch dog for the government to see that the Army does not surreptitiously try to take over civil functions and one of his prerogatives and responsibilities is to see to it that the civil heads of the government have full knowledge of every important cipher or code telegram passing in and out of the War Office. Thus the Permanent Under Secretary of State for War has the right to see all telegrams and can exercise this right through his chief of the code center, who is an old civil servant.

~~SECRET~~

THE MARK VI TYPEX

(Seen on June 11)

On the morning of this date I was afforded the courtesy of examining the new Mark VI Typex machine for field use, the model being at the office of Wing Commander Johnston of the Air Ministry.

The machine is contained in a wooden case approximately two feet long by ten inches deep and ten inches high, the top of which is hinged and can be folded back. On the inside of the top cover are brief instructions for operating the machine; there are also containers for reserve tape reels and a "copy holder". The machine in the case weighs approximately 30 lbs. Power is supplied either from an external storage battery of the 6-volt type usually employed in automobiles or by a set of dry cells delivering approximately the same voltage. This power is used solely for the cryptographic circuits. The actual printing and tape-advance operations are performed by means of a hand crank on the right-hand end of the machine.

The machine can be arranged to be entirely interchangeable in its product with the standard Mark II Typex having five rotors and a reversing wheel. The rotors are, however, of a different type than those employed in the Mark II since the internal wirings are in the form of a "biscuit" or "insert" which can be readily inserted and removed from the core of the rotors. Moreover, these "inserts" are reversible so that the rotors no longer correspond to the type wherein a reverse position of the rotor is not possible (as is the case with the present type of rotors in the Mark II Typex). Each machine comes equiped with a complement of seven such inserts, so that, considering their reversibility, the degree of security afforded by this type of rotor is much higher than with the type of rotor employed in the Mark II machine. The plugboard (for varying the connections in the reversing rotor) is at the left-hand end of the machine, at the base. When I inquired as to whether all the Mark VI machines will

be equipped with this plugboard I was informed that only a few would be, those which might communicate with Mark II machines. It seems that the type of plugs and jacks selected for this purpose is not suitable for field usage, inasmuch as the plugs have a tendency to jar loose. They are not of the type we use (IBM type) and I could see that they would easily come out of place.

The machine is provided with a standard typewriter keyboard which is a duplicate of the Mark II keyboard so that it can be used in the lower and upper case positions. The printing mechanism is at the right of the keyboard and produces a plain text as well as a cipher tape and the characters on the tapes are very large and distinct. Automatic grouping into fives, in the case of the cipher tape, and into the original word lengths, in the case of the plain-text tape, is provided. A locking mechanism insures that only one character will be printed per depression of the key of the keyboard.

When I said that I had been informed that the speed of this machine was 90 characters per minute, Wing Commander Johnston indicated that this was too enthusiastic an estimate and that he rated the capacity of the machine at about 60 characters a minute. I tried out the machine myself and was rather impressed with its ease of operation as well as with its general ruggedness.

The first order of 3900 machines is now in course of production and deliveries are to be begun in November 1943.

A case with spare parts, repair kit, and dry cells, accompany the machine and one man can carry both the machine and the spare-parts case, as a balanced load in both hands.

This machine will no doubt be very useful. It may be interesting to contrast it with our Converters M-325 and M-409. Our M-325 will not produce printed texts but does not require a hand-crank operation; on the other hand it is very much smaller than the British Mark VI Typex. Our M-409 will produce printed text and will be of about the same weight as the Mark VI but will not require hand-crank operation. All three will produce cryptograms of very great security but our devices will be more secure than the British because of the special features incorporated in ours which are lacking in theirs.