TOP SECRET GLINT

CRITICAL OBSERVATIONS

ON

GERMAN TRAFFIC ANALYSIS IN SIXTA

by

Robert G. Nunn, Jr.
Ist Lt., Signal Corps

As a supplement to my report on German Traffic Analysis in Sixta, I submit the following critical observations. My statements of history and opinion are unofficial heresay gathered from casual conversations.

Experience in the German T.A. problem strongly suggest that T.A., Cryptography and Intelligence should be thought of as a single indivisible problem. The processes and products of each one are interdependent and mutually useful to the purposes of the other two. Therefore, the organisation responsible for T.A., Cryptography and Intelligence should be unified at the top and operationally intimate below. This opinion is sgared ny Lt. Col's. Blair-Conyngham and Gadd among others.

A brief account of the history of the growth of Sixta substantiates this observation. During the very early days of the war there was no T.A. done at B.P. Interception control was the responsibility of the Control Department within Hut 6, where an attempt was made to satisfy cryptographic intercept requirements without the benefit of network analysis as it is now known. Intelligence intercept requirements, and the organisation responsible for their fulfilment, developed only after cryptographic success and intercept facilities permitted. Call-sign analysis and the correlation of radio stations with order of battle indentification was at best embryonic.

In 1940 before Dunkerque, a staff in France under Towser (now Col.) and Lithgow (now Lt. Col.) were doing "log reading", though

quite unlike log reading of today. After Dunkerque, Towser went into the War Office with a small group including Blair-Cunynghame, and Lithgow went into the Foreign Office at B.P.

Sometime in 1940-41 Enigma began to be broken on something like a current practical scale. The group under Lithgow devoted itself to correlating order of battle identities from source with call-signs and frequencies and the application of signals information from source to problems of interception. Thus, the present Source Bureau had its beginnings. Nothing like log reading or fusion as they have come to be known was undertaken. However, an occassional re-encipherment was found even without a systematic search.

Independently of the group at B.P. but during the same period, Towser and Blair-Cunynghame in the War Office were developing the processes of systemativ log reading. Training then required only an acquaintance with the "Q" code. Because of the London blitz, this group moved in the early spring of 1941 to Harpenden. There, "log reading" began to come to grips with the problem of continuity. Tracing station continuities without knowledge of call-sign system was the art of log reading. Diaframs of networks began to appear in log reader's notebooks. Another problem presented itself when other intercept stations (Chicksands and Harpenden) in addition to Chatham became operative. This was known as the problem of "reconciliation", that is, comparing and combining logs from two different intercept stations to form a single picture. During the summer of 1941 considerable competition, not always friendly, developed

between the B.P. group and the Harpenden group and the CRR staff at Beaumanor. "Traffic analysis" of the Wehrkreise network was the principle bone of contention. As reports and summaries of their findings began to be published by each, the cryptographers at B.P. principally Mr Gordon Welchman, became interested in possible cryptographic aids to be found from log reading. Discoveries of re-encipherments were brought to his attention by both Lithgow and Blair-Cunynghame. The question of moving the Harpenden group (of the War Office) to B.P. (of the Foreaign Office) was raised but in fact the move was to Beaumanor (by then associated with the War Office) where the combined efforts of the Beaumanor CRR and the Harpenden log readers could be applied to the Wehrkreise problem. the move to Beaumanor was sometime after Beaumanor became attached to the War Office because of the employment of A.T.S. operators and Mr Ellingworth, its head, became a Lt. Col.

After the move to Beaumanor, Thompson (now Lt.Col.) was put in charge with Blair-Cunynghame as his operational chief. There the notion of a Fusion Room develped. However, not all decoded traffic at B.P. was distributed to the "fusion" party. Call-sign analysis, in the meantime, had been developed by the group under Blair-Cunynghame, and the possibility of limited prediction of call-signs was becoming very useful for interception. Late in 1941 the Bird-book was captured in Africa and this knowledge was fully exploited by the Beaumanor group. A weekly W/T.I. report, called "The Beaumanor

Weekly", began to be published, reporting log reading findings network by network, which was the fotrerunner of thr present Sixta Weekly.

Concurrently, cryptographic successes were enlarging, interception was being expanded as quickly as possible (Chicksands was planned by the Air Ministry as an ultra modern fixed station and as such came into operation around January, 1941) and the usefulness of T.A. to both cryptography and interception was suggesting a combined attack, unification. Lithgow's group was continuing to produce signal intelligence, but almos exclusively from source.

Around June of 1943 the Beaumanor group was moved to B.P. largely as a result of the vision and energies of Blair-Conynghame and Welchman. An organisation, called "6 I.I.", was grafted on to Hut 6 with Lithgow at the head, Gadd (now Lt. Col. and the OIC of Sixta) in charge of the original B.P. "source" group, and Blair-Conynghame in charge of the log reading and fusion. Under Blair-Conynghame the proform method of log reading, a more liberal but still limited application of source in fusion process, a routine search for re-encipherments, in short the beginnings of all the basic processes of T.A. - by Sixta as it now is, was accomplished. The security veil between log reading (without source) and fusion (with source) was removed and the integration of log reading and fusion was fostered. However, there remained an organisational division between log and fusion for cryptographic and intercept purposes and "traffic reading" for signals intelligence purposes

Umification was painful and at first avoided for it meant a radical reorganisation in which habits of work would have to be changed.

During the summer of 1943 Blair-Conynghame was called to Africa and Lewis (then Maj. OIC of the Fusion Room, now Lt. Col.) took his place. Gadd continued to direct the "source side" of T.A. And, Lithgow remained at the head of both until around October when he transferred to Hempstead Training Centre. Then, Col. Crankshaw took his place. The lingering organisational division between Gadd (traffic readers, Source Bureau, Liaison Department and M.I.8 Watch) and Lewis (log reading, D/F and fusion) was finally broken down. With the moral support of Welchman, "Sixta" was formed and in November, 1943 Lewis assumed command. The nominal connection with Hut 6 was severed although through the efforts of Maj. Webster, Capt. Rushworth and Fusion Room sector officers, operational intimacy continued to grow. traffic readers moved into the Fusion Room and the basic fusion process of reading traffic in its signals context was begun. The Source Bureau, Liaison Department and M.I.8 Watchg, in short, Hut 3 began to rely upon and in fact applaud the efforts of log reading and fusion. Hut 6 (Cryptography). Hut 3 (Intelligence) and Sixta (T.A.) became operationally unified. In February, 1944 Lewis went to Washington and Gadd became OIC Sixta.

The growth of T.A. under Blair-Conynghame, Lewis and Gadd has involved a series of changes both superficial and radical which have all tended in the direction of the complete operastional integration of T.A. with Cryptography and Intelligence. By degrees, T.A. know-

ledge of networks was accumulated, one by one its applications to cryptography, intelligence and interception were recognised and exploited, though the organisational consequences sometimes caused ill will. Gradually, personnel was recruited and trained, security regulations devised to permit full cooperation and managerial policies were formulated with a view towards maximum individual efficiency, The parts became a whole.

Thus, at the present point in history the integration of T.A., Cryptography and Intelligence no longer appears to be a proposition needing proof, but rather is a basic proposition which may be taken as the criterion of sound policy and efficient organisation.

It is on this basis, therefore, that I submit my critical observations on the policy and organisation of T.A. - by - Sixta.

I. The policy of recruiting personnel for T.A. should emphasize the quality of personnel, not the quantity. Conforming to the usual pattern of history, in the beginning of such an undertaking as T.A., there is available only a very limited number of experienced people. Therefore, from the whole field of possible T .A. functions only the most useful and urgent should be undertaken. As the exploitation of these functions progresses, other possible functions will be recognised by the small but able original staff. Their suggestions for organisational changes and expansion should be encouraged and taken seriously. Only from operational experience canpossible new functions be properly evaluated in the first instance. Once operational opinion is agreed that certain specific undertakings

should be added, the additional personnel should be, as far as possible, chosen and trained by those who have the operational responsibility. In following the above pattern of expansion, the basic idea is to add personnel only because of purposeful conviction on the operational level of the desirability of the expansion and only by means of "hand-picking" with specific jobs in mind. A wholesale creation of a T.A. staff with the a priori idea of providing a sufficienr quantity of people to exhaust the field of T.A. lends to the necessity of susequently culling the unsuited from the staff, which is wasteful and operationally inefficient. On this basis the recruiting policy of Sixta has been altogether commendable.

II. The ploicy on training shoul emphasize individual breadth of view and thoroughness of understanding. every traffic analyst, regardless of how menial his eventual assignment may be, should first be given a course in the practical cryptography relevant to the T.A. with which he will be connected. Following this., he should be given a series of lectures on the intelligence which derives from the cryptographic and T.A. enterprise. The last and probably longest period of his training should be devoted to all aspects of T.A. and the interdependency of T.A., Cryptography and Intelligence. We Americans were given a similar training course upon coming into Sixta. We, therefore, took up our duties with some idea of the ultimate prupose of the tasks assigned to us. Sixta did not, however, provide similar training for previous additions of personnel, althoug the lesson had been learnt by the time of our arrival in October, 1943.

III. the policy on management of personnel should conform to certain precepts. To keep thr "broad view" of traffic analysts alive and to keep them officially informed, not by rumour, of the T.A.-Crytography-Intelligence-contribution to the war effort, periodic lectures should be given by various senior officers in T.A., Cryptography and Intelligence. In Sixta, Fusion Room officers now undertake the major share of this responsibility, however, the need was recognised only after considerable experience.

Again, for the purpose of broadening and deepening their perspective of the problem and understanding of its solution, traffic analysts should be shifted from job to job and department to department as their demonstrated abilities and operational circumstances permit. Although this precept is recognised in Sixta, it is not always urged because of an endemic mon-power shortage. It is a moot point whether or not as much as possible has been done. In particular, Sixta has neglected to urge the rotation of personnel between itself and intercept stations. This is especially valuable for it prevents the thinking of traffic analysts from becoming too removed from the realities of interception.

To insure the maximum individual efficiency, traffic analysts should not only be well informed but also should be allowed the rest and free-time appropriate to the mental facility expected of them. In Sixta, each member is given one day-off a week, which he may take at his convenience with proper notification, and nine days leave every three months, which is assigned in advance by roster. These

matters are left entirely to the operational heads. Non-operational duties of the military staff are minimised.

The final precept of management policy requires that the heads of departments, liaison officers and administrative heads be taken from the ranks of those who began at the bottom.
Throughout Sixta, all Fusion Room officers, heads of departments and the administrative heads proved themselves in the beginning in log reading, traffic reading or similar basic tasks.

IV. The policy on security should emphasize the same idea of a full understanding and practical appreciation of the whole T.A.-Cryptography-Intelligence problem as do the policies on training and management. Furthermore, the daily operational convenience of being able to follow through any chain of analysis to a broken cipher or a useful bit of intelligence should be paramount. In point of fract, appropriate security regulations must be adopted before such ploicies of recruiting, training and management as outlined could be applied. Once we Americans were admitted into Sixta, operational freedom to seek information from cryptographic and intelligence officers was complete. However, only shortly before we arrived had the unveiling occured.

It is submitted that in the above policies the general emphasis on individual knowledge and freedom is a practical corrolary to cooperative endeavor and integrated organisation. Both of which the history of T.A.-by-Sixta demonstrates to be the most suitable forefficient production of military intelligence.

V. Contrary to the previous more or less complimentary references to Sixta, its present organisation contains two undesirable anachronisms which were tacitly referred to in German Traffic Analysis in Sixta, see "...the result of historical growth". (p.45) and "...the methods used (but not by Sixta) are born of T.A." (p.17). I refer to the organisation for interception control and the organisation for sorting traffic both before and after cryptography.

For interception control the organisational division between the Cover Department within Sixta and the Control Department within Hut 6 is, in fact, an artificial distinction between the knowledge neccessary for intelligence control and the authority for assigning intercept tasks. Such a division is useless. And, although from time to time recommendations for a re-organisation are advanced, because of the energies and abilities of Capt. Lovett, head of the Cover Department, the functions of intercept control are so efficiently executed that the need for reorganisation is not operationally urgent. Nevertheless, I believe that Lt. Col. Gadd, in planning the post-war T.A. organisation, regards interception control as exclusively a function of T.A.

For the sorting of traffic both before and after cryptography Hut 6 includes several departments, chief of which are the Registration Rooms and Traffic Identification Section. The former collects, sorts and registers the traffic before the cryptographic attack and the latter purposes -- namely, providing the knowledge of cipher keys upon which the registration Rooms depend, directing the Decoding

Rooms so that messages of a broken key are not overlooked, undertaking "key" and "dud" analyses as explianed in German Traffic Analysis in Sixta, see pp. 56 and 58, and providing general W/T.I. information for cryptographers. These functions all depend upon T.A. knowledge and are frequently accomplished by methods born of T.A.

One of the most strenuous obligations of the Fusion Room is liaison with the Traffic Identification Section in Hut 6. Many times each day discoveries are made or questions arise in both offices which require direct consultation between them. Furthermore the processes and purpose of both offices have so many points of similarity that the division of labor is a hinderance rather than an aid.

For these reasons, it is submitted that the unification of those offices whose function are preliminary and susequent to cryptography is desirable. Either the Fusion Room should move into T.I.S. or T.I.S. into the Fusion Room. Their separation is simply the result of the way they came into being. Their continued seperation is contrary to the rational direction of the development of T.A.-Cryptography-Intelligence towards operational unification.

These observations have a direct reference to the German problem as it is undertaken at B.P., however, they may be understood in reference to any similar T.A.-Cryptography-Intelligence problem, either in war or peace.