OUTLINE OF COURSE GIVEN IN EUROPEAN THEATER
to G-2 PERSONNEL OF 12th A.G., First, Third, Ninth and Fifteenth Armies.

For First Army personnel, this course covered two days. Thereafter it was shortened to one day, encompassing four to six hours of lectures and discussion.

The general outline was as follows:

FIRST HOUR (This generally ran over the time, to maximum of 1½ hours). It was assumed that none of the officers taking the course were cleared for ULTRA material, although in point of fact several officers were cleared, or ultimately cleared, for receipt of such information through their respective SLU's(Special Liaison Units, British staffed, with direct radio communication to the United Kingdom). Only material of CIRO PEARL classification(and lower) was covered, material handled by the U.S. field signal intelligence units. The discussion was opened with a brief summary of signal intelligence successes in the European Theater up to that time. The primary purpose of this introduction was to arouse interest in the subject and to point out that such intelligence could be available for each American Army and Corps.

Then some 15-20 minutes were devoted to a discussion of security, classification and the techniques involved in handling classified material of a Sigint nature. Each student was given copies of the directives governing classification and handling. The meaning of the code words THUMB, PEARL and CIRO PEARL was explained, as well as the significance of "sidelined" entries in routine G-2 reports. Emphasis was placed on the fact that such intelligence could not be disseminated to a level lower than Corps unless its source were disguised.

Primarily emphasis was placed upon the fact that poor G-2 security, or mishandling could effectively compromise the source of the intelligence, and prevent future success.

The following example was used as an example of bad handling:

In 1943, toward the close of the North African campaign, the II U.S. Corps was moving on Biserte. A low grade code message, sent by a German armored division, was intercepted and broken. The message gave details as to time and location for a German attack on the U.S. 1st Division sector. It was broken late. Time was short. The intelligence was passed by radio in an insecure system to the regiment and battalions concerned. The attack failed.

However, from that time on low grade tactical army codes were drastically revised, making solution much more difficult. Throughout the North African campaign they had been a prime source of allied intelligence. In general, it is safe to say that from the time of the Sicilian invasion, a more secure medium grade cipher was generally used for messages of this nature.

QUESTION: Was it better to stem off the attack and compromise the source of the intelligence? Was it better to suffer a setback, and safeguard the source of the intelligence for future use? ~~Discussion followed.~~

This discussion was followed by a brief outline of Sigint techniques as employed in the European Theater:

(1) German callsign systems. A simply worded discussion of the callsign books in use, which assigned "row numbers" to each German unit. (This was naturally eliminated after November 1, 1944)
(2) The significance of this system from the point of view of d/f and traffic analysis. Significant O.B. deductions could frequently be made without cryptanalysis, particularly with mobile formations.
(3) Direction finding. What it could do and what it could <u>not</u> do.

(4) Cryptanalysis. Brief discussion of codes and ciphers in general by the Germans, and how responsibility for solution was divided. Medium grade cipher(double playfair) done at A.G. level and decodes sent forward to armies. Low grade systems(codes, simple substitutions and transpositions, plain text) done at Army and Corps. Decodes sent as far forward as Corps.

.....10 minute break.....

2. 2nd hour.
Specific information as to the units to be allocated to each G-2 taking the course. Tables of organization, names of units commanders. (In the case of VIII Corps and XIX Corps, as I recall, the G-2 staff were not aware of the existence of such units, and had made no arrangements for cross channel lift. In the latter case, the Signal Officer had assumed that G-2 would take care of it. Specific administrative problems and questions were left to the end of the lectures, when all students conferred with Colonel Bicher about these matters.

Following this, students were given a tour of the operations rooms. They started in the teleprinter room, where they could see M serials chalked up on the board and equated with German divisions, and see traffic coming in from the intercept stations. They were shown the map of intercept stations, the D/F stations, and units in training. Then they proceeded to the D/F plotting room. The cue here was to throw in a few words about poor U.S. mobile D/F equipment. Thence to traffic analysis and log reading, where they saw logs of German networks, and network reconstructions based upon the call sign systems previously discussed. Finally, they were taken into the code section, where they saw cryptanalysis in progress. The emphasis here was on the importance of depth. One message in a new system was generally insoluble.

..... 10 minute break .....

3. 3rd hour.
Since at that time traffic analysis, aided by the German call sign systems, was all important, this session commenced with a a reiteration of German c/ss usages, and another explanation of the books. All students given a call sign book to see, and each one looked up a call sign.

Discussion then turned to types of networks used by the Germans. Emphasis here was on "Star"(Stern) and "Line"(Linie), the net types most commonly used from division down. Emphasized the importance of "single call sign procedure" in these systems, in which one call sign only was used for communication between the control or senior station, and the outstation. Showed how easily errors could be made, what sins could be committed by inexperienced intercept operators, how D/F bearings could be made on the wrong station, and how low grade messages, generally unsigned and without address, could be misinterpreted under such a system.

Then each student was given a"canned"problem in network redonstruction. The problem given was one which had actually been done ih operations. A series of messages from networks of the 19th German Air Force Division(approx. 15 in all) compromised the entire division T/O, most unit locations, and the relationship of the units to the "Sector"(ABschnitt) defensive system favored by the Germans for coastal defense units. All errors and garbles were eliminated, messages were carefully translated, and messages with a doubtful direction were eliminated. Map references were inserted in messages.

..... 10 minutes.....

3. Fourth hour.
The entire period was devoted to a discussion of G-2/ signal intelligence unit relationships. Each student was given a list of things which his signal intelligence unit/ would need from him. Emphasis was placed upon the fact that the Signal intelligence unit could not work alone. Without background information, and constant briefing from G-2, the unit could not function efficiently. A partial list follows:
(1) All possible information on Order of Battle and personalities.
(2) Should receive all G-2 reports.
(3) Should have immediate, priority access to all captured documents relating to enemy call signs, frequencies, codes and ciphers, map systems.
(4) Should get a chance at captured enemy signal and cryptographic personnel.
(5) Would be helpful in interrogations of enemy signal intelligence personnel. Would certainly be familiar with techniques and the the language.
(6) Above all, the sigint unit needed G-3 information as well as G-2 information. the intelligence officer can be trusted with details as to intended friendly action. Only in this way can he direct set coverage to get the maximum intelligence for G-2.

..... 10 minute break.....

4. Fifth hour.
Thepractice, the fourth ever generally ran over the allotted time. By this time, the students were apt to be getting tired, but increasingly curious about the results achieved by signal intelligence. By the end of the fourth hour, the whole class was generally grouped about the OB map which SID maintained from Sigint sources alone, talking shop with the instructors. In general, the instructors were enthusiastic about their work, and were apt to"oversell" their product. The final hour of the session was therefore devoted to dampening student enthusiasm and and attempting to secure a somewhat more realistic appraisal of signal intelligence, its advantages, and its more significant limitations. Too optimistic expectations could only handicap the relations which the G-2's were to have with their field units. They would expect the impossible (and in some/ cases, did). The general approach to this problem is outlined in APPENDIX I. In a course such as is proposed in the future, the material outlined in APPENDIX I might perhaps be given somewhat earlier in the course.

5. At the conclusion of the course, all the students met with Colonel Bicher for specific questions as to personnel, the state of unit training, etc.

6. The courses given to First and Third Army personnel lasted two days, and covered approximately nine hours. In these courses, a complete problem was given. Situation reports were prepared, our own troop dispositions were outlined in detail, and "canned" messages covering a three day period were prepared. The exercise was designed to show how signal intelligence could function under ideal conditions. It was felt that this exercise was not overly effective, and it was abandoned.

Material covered on "limitations of signal intelligence". As can be seen, this covered only divisions and below.

Successful signal intelligence work is ~~impossible without~~ difficult or impossible, unless three basic conditions are present:

(1) The enemy will use the radio as a means of communications.
(2) That enough traffic can be intercepted, without excessive garbling or corruption.
(3) That, if code or cipher be used, the systems employed ~~is~~ permit of practical solution, ie, a solution which can be made with available personnel and facilities, in a period of time short enough so that the deciphered material will still be of intelligence value.

This, theme, or variations and elaborations on it, was the basis of the lecture on limitations of signal intelligence. Points covered, as I remember, went about as follows:

(1) Signal intelligence is inoperative and ineffectual if the enemy imposes radio silence.
   a. Where adequate landline facilities exist, radio may be little used.
   b. When such facilities have been overloaded, or rendered inoperative, then a resort to other means of communication(radio) is necessary.
   c. Radio operators and cryptographic personnel require extensive training. It can therefore be assumed that in most instances, some military radio traffic will be found, if only of a practice nature for training purposes.

(2) The European experience was that German armored formations ~~were~~ made far more use of radio communications, than infantry units. Their very mobility ruled out an extensive reliance on static(landline) communications. Very little traffic was taken from infantry type units.
   a. In other cases, where good static communications were lacking(ex. as between 11th Air Force Field Div, on the Greek islands) radio traffic might be extensively employed.(Ditto Jap occupation forces).

(3) It is assumed that sufficient traffic in one cryptographic system can be intercepted, else solution may be difficult or impossible.
   a. Bad atmospherid conditions, unsuitable intercept sites(ex. periodic "blackouts" in Iceland), mountainous terrain limiting factors.
   b. Good security implies the lowest possible power output on transmitters. Good intercept equipment, highly trained and experienced intercept operators a sine qua non. It has been said that through improvement in intercept equipment and aerials, that 50% of the ETO intercept was intercept which was theoretically impossible to copy.

(4) If enemy transmissions are not sent in plain text, then the code and cipher systems used must be solvable.
   a. Certain code or cipher systems are insolvable in theory(one time pads). Other are insolvable in practice(certain types of transposition, Raster a good example). Others, due to the great expenditure of personnel time and machinery involved, can only be handled at the very highest levels

(5) Complex communications procedures daily changing, unsystematic callsigns, changing frequencies, network organization designed to hamper traffic analysis and accurate direction finding- can sharply limit signal intelligence results. The unit network on highest G-2 intercept priority can be "lost" for days if frequencies and callsigns are frequently changes, and if there are no security violations to give a sigint service clues as to the net's identity. German usage of single callsign procedure in many networks sharply reduced the accuracy of allied d/f bearings, and complicated the analysis of message routings.

a. ?Always put in a word about D/F at this point. Many G-2's seemed to have misconceptions as to accuracy and reliability of D/F. Often expected pinpoint locations.

(6) Once intercepted and solved, with an interesting message content, garbles and corruptions can make a message worthless.(See example of corrupt message sent by German 1st Para Army-ULTRA).

(7) Systems which can be read at once may have an intelligence content of no interest to a G-2.

(8) With particular reference to the ETO;---one army or corps unit might be getting a steady flow of intelligence, while its flanking unit got little or nothing of interest to G-2. Both units were experienced capable units. The answer here had to be sought from the German Order of Battle in the two sectors. One unit had opposite it several talkative German divisions, whose communications security was poor. The other unit covered a sector held by security conscious units, which made little use of radio. The Seventh U.S. Army signal intelligence organization, perhaps the best trained and most experienced units in the ETO,always operated under this handicap, while First U.S. Army was never without at least one unit which kept it in business.

~~TOP SECRET~~ REF ID: A671741 ULTRA

SIGNAL INTELLIGENCE SCOOPS FROM THE ETO

1. ULTRA. In the spring of 1944, not long ~~prior to~~ before D-Day, General Guderian, Inspector of German Armored Troops, visited all German armored divisions located in France. A message outlined the General's itinerary in detail. It gave the unit number and location of all the armored formations then in France, as well as the location of some divisional command posts.

2. ULTRA# The counterattack mounted by the Germans against the Mortain-Avranches corridor in August, 1944, was known from signal intelligence sources approximately 36 hours before the blow fell. The attacking forces were known, as well as the areas concerned. As a result, General Bradley was able to make the necessary reinforcements. The attack was made on U.S. VII Corps, including the 4th, 9th and 30th U.S. Inf Divisions, backed up by the 3rd Armored Division and part of the 2nd Armored Division. ~~It failed~~ The breakthrough attempt failed.

3. CIRO PEARL# In January, 1945, during the closing phases of the Ardennes campaign, deciphered messages from a German armored division(Panzer Lehr Division) indicated that (1) it was withdrawing completely from northern Luxembourg, across the Kyll river into the Eifel area of Germany; (2) Only two bridges across the Kyll were intact, one used for eastbound and one for westbound traffic; (3) the divisions refueling points, and ration dumps were specified for a period several days in advance.

Double play

This was concrete evidence that the Germans had given up any hope of further progress in the Ardennes. IXth Aif Force attacks blew the two key bridges. A claim of 1800 vehicles destroyed was made by the air forces.

4. PEARL. During the German retreat across France in August, 1944, the Reconnaissance Battalion of the German 21st Panzer Division ~~acted as~~ frequently the "eyes" for corps and army. Daily it sent back detailed reports to the division command post concerning the sectors held by German infantry divisions, the locations of their command posts, and where main lines of resistance were to be established. These reports were sent in a low grade code, and were generally readable.

Low grade Codes acted as

5. THUMB# In late April and early May, 1944, d/f bearings on an unidentified German formation(using M-35,M-36) showed a move from the Rennes area in Brittany northeastward into the Caen area. Ground sources had carried the German 21st Pz. Div in this area. ~~There had been one reference to a Colonel Hauck who had been reported as commander of one of the Panzer grenadier regiments in 21st Pz Div.~~ The indicated move was reported as a move by 21st Pz Div into the Caen area. ~~This was the first evidence of the presence~~

D/F

Thumb-2 " -1-T/A & P.I.

EXAMPLES ILLUSTRATIVE OF THE LIMITATIONS OF SIGNAL INTELLIGENCE.

(1) Problems arising from corrupt or garbles messages.

ULTRA. In 1945 General Student, Commander of the First German Para Army in Holland, was ordered to mount a counterattack against General Montgomery's northern flank. His reply was interpreted as having read that the area for the attack had been "shifted to the north"(nach Norden verschoben). In reality, the attack had been "postponed until tomorrow"(".auf Morgen verschoben). The corrupt German text, when deciphered, had read as follows:

- Correct Version:	. AUF MORGEN VERSCHOBEN
First Version :	... .A.. .ORD.N VERSCHOBEN
Incorrect Version:	NACH NORDEN VERSCHOBEN

(2)Problems arising from practice or tuning traffic, or traffic sent by the enemy for deception purposes.

CIRO PEARL. Prior to the start of land operations in France, the German Army cryptographic and communications personnel engaged in considerable practice traffic having a spoof content. Fictitious unit names and signatures were used. Most bona fide order of battle identifications had therefore to be accepted with reservation, pending confirmation from other sources. For example, 7 divisions and approximately 15 regimental numbers were mentioned in the practic traffic passed by the 245th Inf. Div in the Dieppe Coastal Sector suring the month of April, 1945.

ULTRA. In 1945, high grade cipher traffic intercepted in Italy contained references to a"LXIII Corps", not previously identified. It was felt that,such was the reliability of ULTRA intelligence, the genuineness of the identification could not be questioned. Only after some time had elapsed was it determined that some of the messages referring to the new corps were prefaced by "tuning message"(Toni Spruch, or Tastspruch), and that the identification was spoof.