WOI Brackenreg

Capt. P. Trost

20/GS Trg Publications/1793

SECRET

THIS DOCUMENT IS THE PROPERTY OF H.B.M. GOVERNMENT, and is intended only for the personal information of

CAPT P. TROST

R. HUST. SIGNALS

and of those officers under him whose duties it affects. He is personally responsible for its safe custody and that its contents are disclosed to those officers and to them only

The document will be kept under lock and key when not in actual use.

1072

SIGNAL TRAINING VOLUME IX

COMMUNICATION SECURITY

PAMPHLET No. 1—GENERAL PRINCIPLES

1948

This pamphlet supersedes Signal Training Pamphlet No. 9, 1944 (Confidential B 951)

Prepared under the direction of
The Chief of the Imperial General Staff

THE WAR OFFICE,
December, 1948

PREFATORY NOTES

Signal Training Volume IX—Communication Security consists of the following:—

Pamphlet No. 1—General Principles, 1948.

Pamphlet No. 2—The Army Code Sign System, 1948. (Confidential B 1598).

CONTENTS

CHAPTER 1.—GENERAL

CHAPTER 2.—WIRELESS SECURITY

CHAPTER 3.—CIPHER SECURITY

CHAPTER 4.—LINE SECURITY

CHAPTER 5.—MONITORING

SIGNAL TRAINING VOLUME IX

COMMUNICATION SECURITY

PAMPHLET No. 1—GENERAL PRINCIPLES

CHAPTER I

GENERAL

SECTION 1.—INTRODUCTORY

1. **Scope of this pamphlet.**—This pamphlet supplements *Signal Training (All Arms) Pamphlet No. 12, Part I—General Principles,* and contains information that cannot be included in that pamphlet for reasons of security. The pamphlet is written for all Royal Signals officers, and particularly for those concerned with the maintenance of communication security.

2. **Communication security.**—Communication security is the protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from a study of communications.

3. **The need for communication security.**—The importance of communication security cannot be over emphasized. It must be realized that in the past the enemy has gained much vital information by intercepting traffic passing over our signal communication system. This has been proved by the study of captured documents. As an example, an extract from a German paper on the interception of our wireless nets in North Africa in early 1943 reads; "During the battle as often before, a considerable carelessness in the use of plain language was noted. Plain language was mainly used for place names. Apart from this, however, matters relative to command and intentions were spoken about with a freedom hardly ever encountered before". That was nearly four years after the outbreak of the war.

4. The enemy may obtain information from all forms of communication for which Royal Signals are responsible. Staff conversations on telephone lines may be overheard by enemy agents; documents may be stolen from signal offices or photographed by agents who may also obtain information that has been disclosed unwittingly by signal personnel; in forward areas, DRs and complete signal offices may be captured. The chief leakage, however, occurs through the interception of wireless traffic; indeed this may often be the principal source of enemy intelligence.

5. **The interception of wireless traffic.**—Modern armies pay great attention to wireless interception, and their intelligence services contain experts who have made a long and detailed study of methods by which the utmost information may be obtained from the most unpromising material.

The basis of wireless interception is the industrious recording of small details. Apparently unimportant details gleaned from our wireless nets, passed back to the headquarters of the enemy intelligence organization, and there combined with similar apparently trivial scraps of information from other sources, build up the outline of a picture. There will be gaps in this picture, and any lapse of communication security, however slight, whether the result of carelessness, ignorance, or the wilful disregard of regulations, may fill in one of these gaps with disastrous results.

The extensive use of wireless makes it inevitable that some information will be given away, especially in battle; security measures aim at reducing this leakage to a minimum.

6. **Security and speed.**—When framing procedure and security instructions, it must always be remembered that the primary function of Royal Signals is to carry our own traffic with the minimum of delay and error. Unfortunately, security measures may impose delays, and the highest possible standard of training for Signals and other users of signal channels is essential if the correct balance between the requirements of security and speed is to be achieved. As stated in *Signal Training (All Arms) Pamphlet No.* 12, the two important considerations are:—

(*a*) The message must reach our own troops in time for them to act upon it.

(*b*) The message must be sent by a sufficiently secure means to ensure either, that the enemy cannot interpret it at all, if he does intercept it, or, that it will take him so long to interpret that its contents will be of little value to him when he has done so.

7. In general, the higher the degree of security imposed, the more complex becomes the method of transmission. In forward areas particularly, occasions may arise when the importance of speed outweighs security. It should, however, be remembered that any relaxation of security measures may give the enemy intercept service valuable help in exploiting other traffic hitherto useless to him.

A rigid code of communication security applicable in all circumstances cannot, therefore, be laid down, and so it is most important that all signal officers should know how leakage of information occurs, and how the security of our communication system can best be safeguarded.

SECTION 2.—RESPONSIBILITIES OF ROYAL SIGNALS

1. CSOs and the senior signal officers of formations are responsible to their commanders for the maintenance of communication security.

Communication security staff officers are included on the staffs of CSOs at all levels, down to and including corps headquarters. They are responsible for advising the CSO and keeping him informed on all matters affecting communication security within the formation. They form a channel for the dissemination of all technical instructions, including those originating from superior headquarters, affecting communication security.

At divisional headquarters, the OC security troop is responsible to the CR Sigs for all communication security matters, except cipher, which is the responsibility of OC cipher troop.

2. The responsibilities of the senior signal officer of a formation include:—

(*a*) The integrity of Royal Signals personnel.
(*b*) Ensuring that all information available to Royal Signals personnel is properly safeguarded.
(*c*) Ensuring that all traffic entrusted to signals is handled in accordance with its security classification. This means traffic handled by regimental signallers, as well as by Royal Signals personnel.
(*d*) The safe custody of documents and secret equipment.
(*e*) Keeping the general staff informed of the state of communication security in the formation, and reporting any particular infrigement of instructions, which may require admonitory or disciplinary action.
(*f*) Issuing instructions (through staff channels if necessary) to all users of signal communications on the security aspect of the communications available to them.

3. **Integrity of Royal Signals personnel.**—CSOs and CsR Sigs will ensure that all Royal Signals personnel are kept aware of the trust that is placed in them and of the heavy responsibility they share for the success of a campaign. Further, OsC signal units are responsible that active measures are taken to detect breaches of trust on the part of those under their command. This applies especially in areas where contact with a foreign civilian population may place temptation in the way of those of weak character.

4. **Safeguarding of information.**—Royal Signals personnel are trusted not to disclose secret information contained in such documents as orders of battle, location lists, and code sign lists, to which they have access in the course of their work. Royal Signals personnel are allowed to handle the plain language texts of all messages except those classified TOP SECRET. None but

specially selected cipher operators may see the plain language text of TOP SECRET messages; orderlies and other personnel not actually employed in transmitting SECRET messages must not be allowed to see the text of such messages.

5. **Despatches.**—SDS traffic often contains TOP SECRET and SECRET information that would be of immense value to the enemy. Royal Signals personnel are trusted to ensure that no despatch handled by them or given into their safe keeping is lost, stolen or captured; and that should the contents of any despatch become known to them the information so obtained is not divulged.

6. **Security classification.**—There must be clear instructions as to how messages of different security classification are to be routed.

These instructions must include details of routing of SDS packages. Besides the danger of capture on surface routes, which may make it necessary to limit the conveyance of packages to those of low security classification, the fact that certain air routes cross enemy territory may mean that only unclassified messages can be sent over these routes.

When checks of traffic are carried out, the routing of messages must be checked to ensure that messages are being despatched by sufficiently secure routes.

Safe custody of documents, signal traffic and equipment

7. The documents mentioned at para 4 above, and any secret equipments must be in the personal charge of the duty signal officer or superintendent, and must be handed over on relief.

8. CSOs and Cs R Sigs, are responsible that clear orders are issued regarding the destruction, as a routine matter, of signal traffic held for specified periods for record purposes, and for the destruction of all signal documents, equipment and traffic should its capture become imminent (*see* Section 6, para 7).

Destruction will only be ordered by an officer, or a warrant officer, who must ensure that everything is destroyed.

CHAPTER 2

WIRELESS SECURITY

SECTION 3.—WIRELESS TRAFFIC SECURITY

Hindering enemy interception

1. While there is always a danger of the enemy intercepting our wireless transmissions, there are two methods of reducing the area in which he can do so:—

(*a*) *Reduction in power.*—By using low power transmitters or in the case of transmitters with a variable power

output, by using the least power that is consistent with reliable communication. This will reduce the ground-wave range of a transmitter.

(*b*) *Very high frequency* (*VHF*).—VHF transmitters have the advantage of being limited in range and aerials can be made more directional at these frequencies.

Even though the fullest use is made of these two means of limiting the enemy's ability to intercept our wireless transmissions, there will remain a very great volume of traffic that he can and will intercept. Security measures aim at preventing him from deducing information from this traffic.

2. **Analysis of wireless traffic.**—The enemy's analysis of our wireless traffic is made more difficult by the use of:—

(*a*) Changing code-signs and frequencies to prevent him piecing together and keeping the wireless picture up to date.

(*b*) Cipher and codes to conceal the contents and addresses of messages.

(*c*) Standard procedure to make it difficult for him to recognize individual wireless stations, links and groups.

(*d*) The link sign system of calling to make it difficult for him to discover the direction of traffic and, therefore, the control station of a group.

Authentication

3. It must be expected that in war the enemy will attempt to intervene on our wireless nets even to the extent of giving acknowledgements and sending bogus messages and orders. It is, therefore, of great importance that a wireless station should be able to determine the friendly or enemy nature of another station. During the last war authentication systems were devised for use when it was suspected that an enemy station was intervening on a net.

The whole subject of authentication is kept under review by the British Joint Communications Board.

4. Further information on subjects related to communication security is contained in other pamphlets as follows:—

(*a*) Change of code signs and frequencies.—

Signal Training (All Arms) Pamphlet No. 12, Part I.
Signal Training Volume IX, Pamphlet No. 2.

(*b*) The use of cipher and codes.—

Signal Training (All Arms) Pamphlet No. 12, Part I, and Chapter 3 of this pamphlet.

(*c*) Security of RT, and codes.—

Signal Training (All Arms) Pamphlet No. 7.
Signal Training (All Arms) Pamphlet No. 12, Part II.

(*d*) Procedure.—

Signal Training (All Arms) Pamphlets Nos. 5 and 7.
Signal Training Volume VIII.

How information is revealed to the enemy

5. **Station and group characteristics.**—Though code signs and frequencies may be changed correctly, standard procedure strictly adhered to, and the link sign system used, the enemy may recognize stations and wireless nets by the following:—

(*a*) The opening and closing of wireless nets at regular times.
(*b*) The morse keying of individual operators.
(*c*) Peculiarities of speech and the use of characteristic jargon on RT.
(*d*) References on RT to previous experiences in other theatres of war.
(*e*) Personalities, ranks, titles, appointments and unit names.
(*f*) The characteristic note of a transmitter.

If, for example, an officer or operator develops a peculiarity of speech on RT, or of operating on WT, it may be possible for the enemy to recognize his unit, and follow its movements.

The reporting of characteristics peculiar to a station or group is one of the functions of monitoring and security sections, for idiosyncrasies which go unchecked may give away valuable information, and undo the results of much conscientious effort in other directions.

6. **Signal activity.**—Line communications are rarely adequate for all speech and message traffic and it is generally necessary to pass a large amount of traffic by wireless. It is impossible to prevent the enemy from studying the grouping of our wireless sets, and the activity on our wireless nets. As far as possible wire-traffic levels should be kept constant by the use of dummy traffic and other deception measures.

7. **Grouping of wireless nets.**—Since wireless stations are normally located at the headquarters they serve, the plan of a wireless net will often give away the level and type of a formation or unit, while the grouping of wireless nets may indicate tactical concentrations.

8. **Direction and routing of traffic.**—Changes in the direction and routing of traffic may reveal movement, or the re-grouping of formations and units. Again, links between formations and

units may be revealed by the routing of the same message over more than one circuit; formation levels may also be disclosed in this way.

SECTION 4.—METHODS OF HINDERING ENEMY DF

1. **Unnecessary transmissions.**—Verbose RT conversations, or the needless repetition of signals, *etc*, make the task of enemy DF simpler. For the same reason, link signs should not be repeated more than twice, and twice only when establishing communication, or when conditions are difficult. Once communication has started to flow easily and smoothly they may be omitted altogether.

If test calls are made during the period when traffic is not being passed, they should be as short as possible, and made at irregular pre-arranged intervals.

2. **Limitation of power.**—The weaker the signal picked up by the enemy station, the less accurate will his DF results tend to be. This is another reason for using the smallest amount of power consistent with reliable communications (*see* Section 3 para 1).

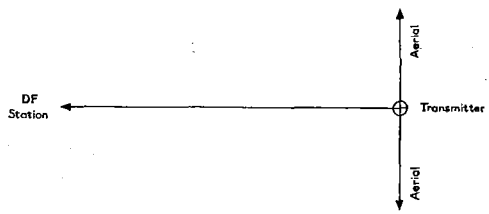

FIG. 1—Use of Ground Aerial.

3. **Ground aerials.**—A ground aerial is very directional. A transmitter with a ground aerial gives bearings of normal accuracy if the ground aerial is laid out on the line joining the transmitter and DF station. The error of the bearing increases as the aerial is rotated, until, when the aerial is at right angles to this line, it will either not be possible to obtain bearings at all, or the weak signals received will make them most inaccurate.

The position of enemy DF stations will not, of course, be known, but his DF will be handicapped if ground aerials are laid parallel to our front (*see* Fig 1 above).

4. **Choice of site.**—Siting wireless stations at a distance from the headquarters they serve is not an effective method of countering enemy DF, unless the distance is so great that it will lead the enemy to search for the headquarters in completely the wrong area.

CHAPTER 3

CIPHER SECURITY

SECTION 5.—GENERAL

1. The object of this chapter is:—

(*a*) To give all signal officers an outline of the general principles of cipher.

(*b*) To ensure that all signal officers have an adequate knowledge of the cipher organization, for the general supervision of which they may be responsible.

(*c*) To ensure that adequate measures are taken to prevent the enemy from obtaining a knowledge of our cipher arrangements.

2. **Knowledge of cipher.**—All signal officers should know the general principles of all grades of ciphers. Details of the higher grades, however, are secret. They are contained in Military Cipher Instructions, which are issued only to holders of the cipher. Only CSOs, officers commanding major signal units, and signal officers and other ranks who have to use, or are responsible for the safe custody of, the higher grade cipher material may see these instructions.

Unit cipher personnel receive instruction in the use of unit cipher only.

3. Authorized users of the higher grades of cipher are forbidden to divulge the methods of enciphering to any unauthorized person. This restriction is binding on them for all time. It still applies when they cease to be employed on cipher duties, and when they are released from the Army.

Authorized users of the higher grades of cipher are also forbidden to discuss cipher matters among themselves in any place where there is any possibility of their being overheard.

Accommodation and safe custody

4. Because the safe custody of cipher and code equipment is of paramount importance CSOs and Cs R Sigs will give the matter their personal attention, and will seek the advice and assistance of local defence security officers regarding the physical security aspect of the problem.

Rooms where cipher equipment is in operation, or stored, or under repair must have securely barred windows, and it must only be possible to enter such rooms through a strong door with a mortice lock.

5. It must be realized that the casual observation and photography of cipher documents and equipment materially assists in the solution of cipher messages. Moreover, there is usually no

evidence from which to suspect compromises of this nature. If such a compromise occurs and the cipher system remains in use, the enemy may be able to decipher *all* traffic sent in that cipher. It will easily be seen that this is far more serious than compromise due to actual loss which can usually be rectified.

Even under field conditions, the cipher office should be allotted separate accommodation, adjacent to the signal office wherever possible. When the cipher office is in a building, care must be taken that it cannot be overlooked from windows, skylights, *etc,* and that it is screened from all observation. If necessary, windows must be stippled or have frosted glass.

6. In large cipher offices, continuous watch will normally be maintained for the full 24 hours. Where this is not possible or necessary the cipher material will be kept in a locked safe, security box or other secure container whenever cipher personnel are not present. The keys of the container together with the key of the cipher office will be kept by the duty signal officer or duty officer, who will be responsible for the safe custody of the equipment during the absence of the cipher office staff. Machines that are unattended must be covered up.

It is most important that secure accommodation should be provided for reserve cipher and code documents and equipment, especially at larger headquarters, *eg,* theatres and commands, where documents and equipment are held some months in advance of the period when they will be required.

7. **Access to cipher offices** will be limited to cipher officers and operators, and to CSOs, communication security staff officers, officers commanding major signal units and such other officers as they may have special reason to nominate. Such nominations (by name and not appointment) will be strictly limited.

Mechanics may enter the cipher office to repair and maintain cipher machines, but they will be under the personal supervision of a cipher operator all the time they are in the cipher office, and he will ensure that they confine their attention to their work. They will not be allowed to handle the secret components of cipher machines, except to repair or adjust them.

8. **Duty signal officers.**—Duty signal officers unless specially nominated are not allowed to enter the cipher office, nor to watch cipher work in progress. They must, however, watch the routing of traffic to avoid cumulative delays in the cipher office, and they must know the rate at which cipher operators can handle traffic. The average speed for enciphering and deciphering is as follows:—

Machine ciphers	10-12 groups per minute.
Book ciphers	3-4 groups per minute.
Unit ciphers	2-3 groups per minute.

These are overall times, covering preparation of apparatus, completion of the message form for despatch, registration, *etc.* When deciphering, however, these speeds can be maintained only if a message is free from corruptions. Corruptions are frequently due to errors in transmission. The more serious they are, the more time is taken in solving them.

SECTION 6.—SECURITY OF CIPHER

1. The term *security* (as distinct from safe custody) when applied to a cipher refers to:—

(*a*) Its inherent resistance to organized cryptanalysis.

(*b*) The observance of the correct method of operating and handling the cipher.

(*c*) The control of the amount of traffic passed in each cipher to ensure that its *safe life* (*see* para 5 below) is not exceeded.

2. **Resistance to cryptanalytical attack.**—The inherent resistance of a cipher to cryptanalytical attack depends on the complexity of its construction. This does not mean that a very secure cipher is necessarily slower to operate than a less secure one.

3. **Handling of wireless traffic.**—The secure handling of wireless traffic and the secure use of ciphers interlock very closely in practice, for the cryptanalyist is aided in his task if he can discover the identity of the addresses of a message, or even the level at which a message has been transmitted.

An insecure system of handling wireless traffic thus damages cipher security.

4. **Handling of ciphers.**—Enciphering is not simply a matter of copying groups from a vocabulary book or pressing the keys of a machine; it is a task that can be performed efficiently and safely only by a trained and experienced operator.

5. The security of any cipher is in inverse ratio to the amount of traffic passed in it. Any cipher system, if used to excess without a change of key, will reach a point where its degree of security will begin to diminish rapidly and progressively. For this reason the maximum number of groups that may be safely passed in any one cipher key is limited; the number of groups which is permitted is termed the *safe life* of the cipher concerned.

This feature of the use of cipher explains the absolute necessity for the prompt rendering of traffic returns. Some ciphers have many users, and unless the amount of traffic passed in them is constantly watched by means of consolidated returns, it is impossible for cipher security staffs to know when the safe life of a cipher is nearing its end.

6. **One Time Process (OTP) cipher.**—As its name implies OTP is a type of cipher that is used once only; if it is correctly used, it is absolutely secure.

It is used for certain messages of high security classification, and also for messages, whose text may have to be published later. OTP is the only suitable cipher for the latter class of message because the possession of the plain language version can then be of no possible help to the cryptanalyst in solving other messages.

Although from the security aspect, the exclusive use of OTP cipher would be ideal, this is not practicable, because of the amount of equipment involved. The use of OTP cipher will, however, be extended in the future and already several links of the Army Wireless Chain employ OTP for all cipher traffic.

7. **Compromise of cipher.**—Every effort must be made to prevent the capture of cipher documents by the enemy. Possession of cipher keys will enable the enemy to read all messages that have been sent in those keys. When the capture of a headquarters appears imminent, all cipher equipment must be destroyed. Any loss of equipment, compromise or suspected compromise, or the destruction of equipment in an emergency must be reported to the next higher authority as early as possible.

The higher grades of cipher entail complicated equipment and elaborate documents which take time to produce. This equipment, and these documents must not, therefore, be exposed to the risk of capture, because of the difficulty of replacement.

Except in the case of OTP unauthorized persons should never be allowed access to the clear version of a cipher message.

SECTION 7.—TECHNICAL RESPONSIBILITIES OF COMMUNICATION SECURITY OFFICERS

1. A Staff Officer (Communication Security) is responsible to his CSO for:—

(*a*) The technical training and efficiency of all concerned in the use of ciphers and codes (SLIDEX, map reference codes, state codes, air support control codes, *etc.*).
(*b*) Complying with technical security instructions.
(*c*) Distribution, safeguarding and destruction of cipher and code material in accordance with current instructions.
(*d*) The preparation, issue and change of cipher and code keys and settings.
(*e*) Issue of code signs.
(*f*) Authentication systems (*see* Section **3**, para 3).
(*g*) Cipher traffic returns.
(*h*) Wireless security measures.
(*j*) Advice and assistance to all subordinate formations on communication security problems.

At divisional headquarters these duties will be shared between the OC cipher troop and OC security troop as appropriate (*see* Section 2, para 1).

Correspondence

2. Staff Officers (Communication Security) and cipher officers when signing correspondence will do so " for " the CSO or CR Sigs. Similarly, all correspondence, and cipher material not passed by hand, will be addressed to either the CSO or CR Sigs.

3. Correspondence of a non-technical nature, *eg*, concerning the supply of non-technical equipment, including Typex machines, the provision, posting and promotion of cipher personnel or changes of establishments, will be dealt with through normal channels in accordance with its security classification.

4. For security reasons it is essential that knowledge of all technical aspects of cipher should be restricted to those who require it to carry out their duties. Cipher documents not passed by hand and correspondence on all technical cipher matters will, therefore, invariably be enclosed in two envelopes, the inner one being sealed and marked as follows:—

(TOP) SECRET	(TOP) SECRET
CSO (CIPHER) *Formation*	CR Sigs (CIPHER) *Formation Signal Regiment*
OR	
This package will be passed UNOPENED to the addressee or the Staff Officer (Communication Security).	This package will be passed UNOPENED to the addressee or the Cipher Officer.

Arrangements will be made that packages so addressed are NEVER opened in formation registries or formation signals orderly rooms.

Access to, and handling of, technical cipher correspondence files must be strictly limited.

5. At establishments where there is no CSO or CR Sigs the foregoing rules will apply except that packages will be addressed to, and correspondence signed " for ", the head of the establishment.

At brigade level, communications will be addressed to the brigade signal officer. Correspondence on technical matters will be addressed as laid down in para 4, the words " Brigade Signal Officer " and " Cipher N.C.O. " being substituted for " CR Sigs " and " Cipher Officer " respectively.

At unit level communications will be addressed to the commanding officer.

6. In practice, it will often happen that the staff officer (Communication Security) or cipher officer initiates, opens and deals with technical cipher correspondence. It is, nevertheless, his responsibility that the CSO (or CR Sigs) and other Royal Signals branches, when necessary, are kept fully informed and up to date on cipher matters.

CHAPTER 4

LINE SECURITY

SECTION 8.—ORIGIN AND DEVELOPMENT OF LINE SECURITY

1. **Categories of line.**—From the point of view of line security, lines may be divided into the following main categories:—

(*a*) **Field lines,** which are lines at and forward of the headquarters of a division engaged in active operations.

(*b*) **L of C lines,** which include all military or civil routes used for military traffic from the headquarters of the theatre as far as the headquarters of divisions taking part in active operations, and all the lines without exception of an army occupying an ex-enemy country.

Historical

2. The trench warfare of the war of 1914-18 lent itself admirably to line interception.

Extensive line networks were developed particularly in the forward areas adjacent to no man's land, and as there was then little wireless in field formations these line networks were the principal method of communication.

3. In the first years of the war the line security of the Allies was incredibly bad, and there is no doubt that the enemy, who had a well-trained and well-organized interception service available from the beginning, obtained much valuable information from telephone conversations that he was able to intercept.

Telephone users could not be made to understand that the enemy might be listening to all that they were saying, and our intelligence service failed to realize what could be achieved by intercepting enemy telephone conversations.

4. It was not until several disasters in the autumn of 1916 had been directly traced to the leakage of information on telephone lines, that the vital importance of line security was realized.

The reaction was violent, and for a time officers mistrusted the telephone, and were reluctant to use it at all for fear of what might be given away, but the result was that in the last two years of the war efficient line security measures had been worked

out, and were being strictly enforced. The fullerphone was in general use, all messages bearing a security classification were being enciphered, and code names were being used in plain language conversations.

5. Since 1919, the extensive use of wireless in military communication has meant that wireless security has taken priority over line security, but this in no way diminishes the vital importance of the latter. This was clearly established in the war of 1939-45, when the Allies found it necessary to organize special monitoring sections to raise the standard of line security, and investigate how leaks of information were occurring.

Section 9.—METHODS OF LINE INTERCEPTION

Field lines

1. It is in defence that the possibilities of line interception are greatest. The attacking forces use the telephone incessantly and become careless in what they say. This gives the defending line intercept organization an excellent opportunity of discovering the plan of attack.

2. In forward areas the normal method of line interception is by induction from earth return lines.

A long line, normally of field cable, is run out as far as possible toward or into the enemy line network. At the far end the line is earthed, and an amplifier is connected to it to increase the power of the weak induced signals.

The line is usually laid by a member of the line intercept organization, who joins a patrol for the purpose The patrol guides him through the enemy defence works, *eg,* minefields, barbed wire, *etc,* thus enabling him to penerate to the maximum depth. The maximum range of this type of equipment is 3,000 yards from the point where the amplifier is connected.

3. The occasions on which this method can be successfully employed in forward areas without undue risk of detection are obviously limited, but there is evidence to show that the Germans used it with good effect several times during the Italian campaign of 1944-45. As an auxiliary component of the amplifier, they fitted a piece of equipment that could be placed on the enemy line itself without disturbing its electrical characteristics.

One particular incident was at Cassino early in 1944, when, because of the peculiar nature of the front, the enemy were able to " tap " a line from an Indian brigade to its divisional headquarters.

4. It is possible to use unbroken railway lines, intact underground cables, metal pipes and other conductors instead of the earth intercept line, and there are a number of cases on record of this having been done successfully.

L of C lines

5. In L of C areas, the most fruitful source of information is agents, who are either employed in civil exchanges, repeater stations, *etc,* or who tap military circuits.

Circuits may be tapped either outside or inside exchanges, *etc,* but if they are tapped inside the tappings are easier to conceal, they can be made more permanent, and it is easier to tap busy trunk lines on which important information is passing continually.

Information obtained from tapping circuits is either taken down by the agent, or recorded on an instrument such as the magnetic wire recorder.

SECTION 10.—COUNTER MEASURES AGAINST LINE INTERCEPTION

Field lines

1. As the basis of line interception is induction through the earth, the most effective counter measure is obviously to have nothing but metallic circuits within 3,000 yards of the front, but for tactical reasons this may not always be possible.

2. Where it is not possible to achieve a line system wholly of metallic circuits in a forward area, the scope of the enemy's line interception may be reduced by the following precautions:—

(*a*) The number of lines running from company headquarters to outposts and platoons should be reduced to a minimum.

(*b*) All earth return circuits should be graded as unclassified.

(*c*) An experienced regimental signaller should patrol forward lines frequently, his tasks being to:—

(i) examine lines for evidence of tapping.

(ii) repair or replace portions of the line whose insulation is deteriorating.

(iii) reconnoitre unaccountable lines, and look for other evidence of possible enemy intercept lines.

(*d*) Party lines should be avoided whenever possible.

3. Experiments were made in Italy in 1945 with an oscillator which was specially designed to saturate stray alternating speech currents without impairing the efficiency of our own telephony network.

These experiments were reasonably successful, but no equipment has yet been developed for use in the field.

L of C lines

4. Close contact should be established with the civil police, and the appropriate civil authorities, who should be asked to produce the records of all civilian employees concerned in the operation of the communciation system.

Any employee about whose integrity there is the least doubt should be dismissed immediately, and if employees whose records are satisfactory act suspiciously the civil police should be asked to pay surprise visits to their living quarters and search them.

5. The possibilities of tapping circuits inside a terminal office or repeater station, *etc,* or on an intermediate frame or terminal strip are many and varied, and a frequent and thorough inspection of all circuits and related equipment is necessary to prevent it being done. Such an inspection will soon reveal any redundant or peculiar circuits and equipment.

In buildings

6. In general the following points should be looked for:—

(*a*) Splices and bridges in jumper runs.

(*b*) Small cables leading to special rooms, or leading outside a building. They may be connected to monitoring or recording equipment.

(*c*) Rooms which have monitoring or recording equipment in them, such as amplifiers, head-phones or automatic recorders.

(*d*) Any suspicious or apparently surplus equipment.

(*e*) Small condensers, or resistors, or a combination of both around terminal blocks, *etc.* They may be used for high impedance bridging.

(*f*) Any VF telegraph channel filters or demodulators which might be used for intercepting VF telegraph signals.

(*g*) Small portable recorders and any such equipment in all parts of the buildings concerned, including the living quarters of civilian personnel.

7. In addition the following points should be checked:—

(*a*) All lines or cables which lead into enemy or neutral territory to ensure that they are disconnected, bunched and earthed.

(*b*) All records of daily line tests. These should reveal any suspicious change in the characterisics of any line. The line concerned can then be checked in detail for the cause.

(*c*) Switchboards for unnecessary wiring. Particular attention should be paid to long distance, trunk and the more important local lines.

(*d*) Intermediate and main frames, and other similar equipment for terminating or re-distributing lines, to ensure that no surplus tappings exist.

(*e*) Repeater stations and other buildings used in conjunction with the lines and line equipment for unaccountable wiring or equipment.

External routes

8. Frequent patrols along external routes reduce the possibility of casual interception by the enemy. Continuous interception of outside routes requires very elaborate arrangements, and it should be easy to trace these. Some suggested checks are as follows:—

(*a*) Signs of trenching on cable or overhead routes that might indicate that a tee-in cable has been installed.

(*b*) Clues in the neighbourhood of test points or terminals used by line parties.

(*c*) Any kind of wire in the neighbourhood of a cable or open wire route. If the wire leads to a building, inspect the building.

(*d*) In towns, examine manholes and cable-chambers for the presence of unaccountable lines connected to main cables at the jointing sleeves.

(*e*) In occupied countries, ask civilians if they know of any suspicious persons in the neighbourhood. A few enquiries in the course of routine patrols often result in a whole village becoming permanently "spy-conscious". If interception is suspected, house-to-house searches should be made.

(*f*) Maps of enemy cable systems should be examined for records of old tee-in cables. These cables should be traced on the ground to their termination.

9. **The security classification of lines.**—Rules for the security classification of line circuits are given in Section **11**.

Messages which have to go over a circuit of a lower security classification than themselves must be enciphered.

SECTION 11.—SECURITY CLASSIFICATION OF LINE CIRCUITS

1. The basic principles set out in this section are a guide to the security classification of line circuits.

2. **Secret.**—Line circuits may be classified Secret only if they fulfil the following conditions:—

(*a*) *Equipment and terminal conditions.*

(i) The system employed comprises either:—

Teleprinter or telegraph circuits on carrier channels, *or*

Teleprinter or telegraph circuits wholly within an adequately guarded military reservation, *or*

Telegraph circuits not employing audio frequency alternating currents (*eg,* fullerphone), and

(ii) All repeater and terminal equipment involved is under complete military control and restricted to authorized military and civilian personnel, and

(iii) Opportunities for multiple appearances of clear text, such as switchboards and distributing frames, are kept to a minimum and are safeguarded against connection to unapproved circuits or unapproved local lines, and

(iv) All terminal equipment is operated by authorized personnel.

(*b*) *Circuit conditions.*

(i) The circuits (other than those wholly within an adequately guarded military reservation) are subject to visual inspection for their entire length and are under frequent ground patrol. (Visual inspection of the ground over buried line will fulfil the requirement for such lines), *or*

(ii) Circuits enclosed in a metal sheath which is filled with gas under constant pressure with all joints sealed, *or*

(iii) Submarine cable circuits, which meet the requirement in (i) above for their land line portions and the submarine portions of which are located in sea areas patrolled by British forces and nominally controlled by them.

3. **Confidential.**—Line circuits may be classified Confidential only if they fulfil the following conditions:—

(*a*) Circuits which are located in an uninhabited area or an area occupied by allied military forces whose inhabitants are friendly or co-operative or who, for all practical purposes, are without technical knowledge in the communications field, and the terminal conditions of which meet the requirements of para 2 (*a*).

(*b*) Submarine cable circuits which conform to the provisions of sub-para (*a*) above for their land line portions and the submarine portions of which are located in areas patrolled by British or Allied Navies and nominally controlled by them.

4. **Restricted.**—Line circuits may be classified Restricted only if they fulfil the following conditions:—

(*a*) Teleprinter or telegraph circuits using wire facilities exclusively and operated by personnel under control, or subject to the supervision of military personnel, or, in tactical conditions, any electrical communication.

system using wire facilities exclusively (*eg*, telephone or buzzer) which is not liable to enemy interception.

(*b*) Commercial teleprinter circuits when the originating and terminating printers are operated by authorized personnel.

CHAPTER 5

MONITORING

SECTION 12.—GENERAL

Communication security and monitoring

1. The maintenance of communication security depends mainly on three factors: technical measures to defeat interception, the design of secure procedure, and strict adherence to these procedures by all users of the communication system. It will be seen that for the last two, continuous observation of the communication system is essential. Thus monitoring, or the recording and examination of traffic on line and wireless systems, is an important aspect of communication security.

Objects of monitoring

2. The objects of monitoring may be summarized as follows:—

(*a*) To check that security instructions and correct procedure are being strictly adhered to.

(*b*) To reveal security weaknesses in current procedure with a view to its redesign.

(*c*) To assess the state of security in any particular formation or on any particular system.

3. Security monitoring may also contribute directly to the efficiency of the communication system in that difficulties and causes of delay may often be revealed. Such information is of great assistance to those responsible for traffic handling.

Responsibility for monitoring

4. It is the responsibility of Royal Signals to ensure that secure communications are provided. The effectiveness of security measures can normally be assessed only by constant monitoring and the responsibility for this also rests with Royal Signals.

Monitoring personnel either form part of security troops of divisional signal regiments or are attached to signal regiments of higher formations.

SECTION 13.—WIRELESS MONITORING

General method

1. Wireless monitoring is at present concerned only with hand-speed WT circuits and RT links. The method is as follows. Monitoring operators using wireless receivers prepare a log of the traffic passing on a circuit. This log is then examined by a communication security officer whose duty it is to pass the results of the monitoring to those concerned, so that the lessons may be learned and the general standard of security raised (*see* Section 15).

The monitor log

2. The log prepared by a monitor operator is not simply a record of the traffic passed on a circuit, but must contain details of every transmission, together with notes on the following subjects:—

(*a*) State of communication (signal strengths, interference, *etc*).
(*b*) Standard of operating.
(*c*) Maintenance of correct frequency.
(*d*) Supervision by "control".
(*e*) Characteristics of officers and operators on RT and operators on morse.
(*f*) Characteristics which would help to identify the circuit.
(*g*) Set characteristics, *eg*, peculiar background noise.

3. When monitoring WT, a good operator will be able to take down every transmission including all procedure and operating signals, repetitions and corrections, *etc*. On RT it will often be impossible for an operator to record every conversation verbatim. In these circumstances the log must show the gist of conversations and, in particular, any passages in code. The log must be amplified by notes on procedure, verbosity, *etc*.

The monitor operator and his duties

4. The preparation of a log as described above requires a specially trained operator who, apart from his ability as a wireless operator, must have a clear idea of the objects of monitoring and the use to which the log is put. He must be able to read morse well through interference, possess a sound knowledge of WT and RT procedure and RT codes, and be able to write quickly and legibly.

5. He must enter personal observations on the log as he goes, drawing attention to breaches of security and procedure by underlining or marginal notes, and must sum up in an "end of watch" criticism.

6. He must refer urgent breaches of security to the NCO in charge at once.

7. Ideally, a monitor operator's log should be ready for examination as soon as his watch is finished, although it may sometimes be necessary, particularly in the case of RT monitoring, for him to make a fair copy of it.

8. It must be appreciated that the work of a monitor operator is extremely arduous and for this reason, watches must be short.

Examination of the log

9. The monitor log is passed to the communication security officer for examination or it may be submitted to him through a NCO who will prepare a brief report on the log.

SECTION 14.—LINE MONITORING

General

1. Line monitoring is mainly concerned with telephone conversations, since it is with this form of communication that users are most careless. Although there are fewer possible breaches of security and the risk of interception is less than on wireless, constant supervision is necessary to ensure than an enemy cannot gain information.

Method

2. The usual method of telephone monitoring is similar to wireless monitoring in that monitor operators prepare reports for examination by a communication security officer.

3. Best results may be achieved by employing shorthand-typists who are able to take down conversations word for word. They then prepare a précis of each conversation for the communication security officer. The latter is thus able to examine the subject matter of many conversations, and to call for a verbatim transcription of any conversation, which appears to have infringed security.

4. For recording particular breaches of security and for monitoring when shorthand-typists are not available, excellent use may be made of the magnetic wire recorder. As a monitoring device the wire-recorder is also most useful in that it provides the facilities of a normal amplifier and gives reception via loudspeaker or headphones.

5. Monitoring is best carried out in a room or vehicle adjacent to a telephone exchange. Tappings on the test frames will give access to any circuit and by using a number of leads and a suitable arrangement of plugs and jacks at the monitor position, each operator may select any one of (say) five circuits which have been tapped.

SECTION 15.—RESULTS

1. On his examination of the wireless log and telephone monitoring reports the communication security officer will take action which will normally fall under one or more of the following headings:—

(*a*) Submit to the senior signal officer of the formation a report on breaches of procedure and recommendations for training or improvement in procedure.

(*b*) Submit a report on breaches of security for the information and guidance of those concerned and, in certain cases, for disciplinary action to be taken against the offenders.

(*c*) Prepare periodically, for the senior signal officer, and the general staff, reports on the standard of wireless security throughout the formation.

(*d*) Prepare consolidated reports for higher formation.

(*e*) Ensure that the general staff is informed immediately of any serious breach of security. In extreme cases a change of operational plan may be necessitated by information having been given away and no time must be lost in bringing this to the notice of the staff concerned.

(*f*) Maintain records so that information on the standard of procedure and security in the various units and formations is readily available.

(B48/469) 1700 6/49 W.O.P. 30492

SECRET