Pamphlet No. IV

SECRET COMMUNICATIONS

It is quite obvious to all of us that we have to discuss the various methods of secret communications seriously. We realize that,,as our groups grow and spread, we will find it necessary to transmit messages, reports, instructions etc. from group to group. We have to beware that if these messages are intercepted and read, the whole organization will be endangered. Later, in the event of active hostilities, it will become even more urgent to send messages safely, speedily and secretly.

For this purpose we have made a study of the many methods of secret communications and have come to,the conclusion that the following merit closer consideration. 1) Codes 2) ciphers 3) secret ink and 4) secret methods of delivery. Let us deal with eachmin turn.

I) CODES: Codes are really billingual ddictionaries i.e. letters or signs are used to represent other letters, words or ideas eg. the morse code. Here letters pf the alphabet are indicated by variations of dots and dashes. The various commercial and military codes follow the same principle except that, in most cases a sign represents an idea or a word. (cf. the local road signs)

For our purpose codes have the following advantages:- 1) they offer maximum security in that they are difficult to decipher unless the code book lands in enemy hands or the enemy intercepts a number of our messages.
2) They are quick and simple to encipher and decipher which reduces the margin of error and also saves time especially where speed is essential.
3 Despite these obvious advantages, however, codes have the following staggering disadvantages:- 1) There are obvious limitations on words and serviceable sentences. Only those words provided for in the code book can be used.
2) Codes cannot be changed or replaced at a moment's notice. This means that if the code book falls into enemy hands, much time is lost in working out and editing a new book.
3) Once the code book is captured by the enemy much damage can be done if we are unaware of the fact.

II) CIPHERS: Ciphers are secret writings in which any idea or message can be written. It is not limited, as is the case with codes. No dictionary is necessary. All one needs is a key. We are more interested in ciphers therefore, as we envisage carrying extensive communications which will entail frequent changing of ciphers for the sake of security. Before we discuss the various types and variations of ciphers, we should bear in mind the fact that a good cipher should fulfil the following requiremen ts:- a) it should be relatively simple to encipher and decipher. This would eliminate the possibility of error. b) it should be reasonably quick to encipher and decipher. This will become more important when the message is urgent. c) it should, if possible, be above suspicion. In other words, it should not look like a cipher. This would increase the chances of success.

There are two basic types of ciphers viz. a) Transposition and b) Substitution ciphers.

a) Transposition Ciphers: Transposition ciphers are formed when the normal position of the units making up the message in plain reading, are changed eg. writing the message backwards. N.B. The original letters of the message are maintained. They are only scrambled according to some method.

Two methods of scrambling the letters are by using a) Geometric patterns and b) Route Transcription

(a) Geometric Patterns:-

A message containing, say, 20 letters can be written vertically in two columns of ten letters each and transcribed horizontally in groups of 2,4,or 5. The group lengths are quite arbitrary. A me message of 16 letters, for instance, lends itself easily to groupps of 2,4,8, (2x8; 4x4; 8x2).

The most common geometric shapes are squares, rectangles and triangles. More elaborate shapes are subject to error. e.g.
Message in plain text:EXPECT ME SATURDAY NOON. (20 words).
Written vertically:- EX
PE
CT
ME
SA
TU
RD
AU
NO
ON.

Transcribed:9group lengths of 4)
EPCM STRA NOXE TEAU DYON.

(b) Route Transcription:

Route transcription is done in blocks which are read either vertically, horizontally or spirally.
Here it is best to give examples:

(horizontal)	(vertical)	(spirally-clockwise)
SECRE	S E M I I	S E C R E
TCOMM	E T T M C O	S N O I T
UNICA	C C U A N	I C A T C
TIONS	R O N T S	N J M M O

From these examples it is obvious that many variations may be developed, It is always wisest, however, to keep to the simpler forms to avoid error and delay.
Note: Before enciphering a transcription cipher, we must determine the following:-
(a) Size and shape of geometric pattern.
(b) Starting place and route.
(c) Group lengths.

* Grills:

This is really a form of transcription cipher. Here perforated cardboard matrices, called grills, are used. These perforated plates are placed on paper and the message written in the holes. When the cardboard is removed, the remaining space on the the paper is filled with meaningless letters. This type of secret writing entails carrying a grill on one all the time as no message can be read without the perforated cardboard. As is the case with codes, this is a simple quick method of sending messages. The main danger here. again, is that the perforated board might be seized by the enemy.

II. Substitution Ciphers:

These differ basically from transposition ciphers in that th different letters or signs are substituted for those in plain text. A very simple form of the substitution cipher is writing down the alphabet in the conventional manner and then writing a reversed alphabet below it. The reverse becomes the cipher - in other words z = a and y = b. This can be varied by changing the starting point of the alphabet or by using 2 or more cipher alphabets.

Mixed Ciphers:

This best explained by example. Here a key word is used as the starting point of the cipher alphabet. We will use the word"Cipher".

A B C D E F G H I J K L M N O (etc)
C I P H E R A B D F G J K L M (etc) Omitting those letters contained in "cipher".

DECODING:-

We must always bear in mind that experts can determine, by means of frequency tests, whether transposition or substitution have been used, because of the frequency with which certain words or letters (in any language) occur. They can break any code or cipher - given time. It is for this reason that ciphers used, have continually to be changed.

III. Secret Ink and Other Secret Methods:-

Codes and Ciphers are not the limits to secret communication. Secret inks are invaluable especially if one wishes to avoid suspicion. Inks that have been used for this purpose are:-

(i) Chloride of Cobalt solution (ii) Oil of Vitriol , (iii) Onion , (iv) Vinegar (v) Ammonia - (They all become visible on heating)
(vi) Alum Solution (becomes visible when moistened).

Other disguises include sending messages in newspapers (marked with secret ink) on wrapping, clothing etc .

IV. Methods of Delivery:-

Here we may consider:-

(i) Postal Service: (wherever it is safe).
(ii) By Personal Contacts. Here people who could be used include commercial and other regular travellers, students, visitors.

Note well: It is essential that all contacts be above suspicion.

IMMEDIATE PROBLEMS:

(i) Deciding on which codes or ciphers to adopt.
(ii) Acquainting ourselves with the basic principles of codes and ciphers.
(iii) Instituting a regular exchange of newspapers.
(iv) Working on a suitable ink.