Army Code No
PROM 401

The Information given in this document is not to be communicated, either directly or indirectly, to the press or to any person not authorized to receive it.

ENGRS/SIGNALS/INTELLIGENCE & MP

CAPTAIN TO MAJOR WRITTEN PROMOTION EXAMINATION
DIRECT REGULAR COMMISSION OFFICERS

Prepared under the direction of

Chief of Army Staff

2023

NOTE

Any Mistake, Omission and Advice on the Module should be forwarded to :

THE COMMANDER
HQ TRADOC,
NA MINNA.

TABLE OF CONTENT

CMWPE MODULE ON MILITARY TECHNOLOGY FOR NAE

INTRODUCTION

1. Candidates sitting for the CMWPE are required to be capable of commanding an Engr Fd Sqn in battle. To achieve this, they will therefore be required to understand the employment of an Engr Fd Sqn in battle, the roles of NAE in assisting the NA to live, move and fight and specially in supporting the Army in the contemporary operations.

AIM

2. The aim of this precis is to provide adequate guidelines required by candidates sitting for CMWPE Examination.

SCOPE

3. In preparation for these guidelines, references were made to the existing materials that relate to the contemporary challenges facing the nation. For easier understanding and better assimilation of the subject, this precis is rearranged into the following topics:

a. The roles of the NAE and the principles of employment.
b. Reserved Demolitions.
c. Oppose River Crossing Ops.
d. Bridging.
e. Improvised Explosive Device and Explosive Ordnance Awareness and Recognition.

4. The topics discussed have been selected for the purpose of the CMWPE Examination in Military Technology only. They are in no way exhaustive of the roles and capabilities of the Engineer Corps.

CHAPTER ONE
THE ROLES OF NIGERIAN ARMY ENGINEERS

INTRODUCTION

1. Combat Engineer Units are those NAE units found in field formations. They act in support of the comd's tactical plan and are often found grouped with other arms. When so employed, the works they carryout are termed combat engineering.

2. This chapter outlines the main roles of the combat engineers across the spectrum of conflict which include:

   a. Mobility Support.
   b. Counter-Mobility Support.
   c. Survivability Support.
   d. General Engineer Support.

MOBILITY SUPPORT

3. Combat forces require the ability to manoeuvre rapidly and freely on the battlefield. Mobility is necessary to achieve concentration of effort and to deploy rapidly to engage or to disengage from the enemy. Superior mobility may compensate for numerical inferiority. Terrain, weather and enemy activity will affect mobility of battlefield.

MAIN ENGINEER MOBILITY TASKS

4. In supporting the mobility of all arms, the main engineer tasks are:

   a. Gap crossing including wet and dry gaps.
   b. Countermine operations which include detection,

reconnaissance, marking, bypassing, breaching and clearance of mined areas.

c. Counter obstacle operations which include breaching, bypassing or reduction of obstacles other than gaps and mined areas.

d. Development and improvement of routes for tactical movement.

e. Support to forward aviation task which may include the construction, repair and maintenance of forward airstrips and the preparation of landing areas.

COUNTER-MOBILITY SUPPORT

5. Counter-mobility operations disrupt an enemy's manoeuvre plan and deny him the use of terrain. They may also reduce the effect of an attacker's superiority in numbers, and channel him into and retain him in areas where he can be defeated. Counter-mobility planning must also take account of own force manoeuvre requirements. It must be correctly balanced so as to disrupt the enemy's mobility while limiting the restriction on our own. It is particularly important that likely tasks and moves for own forces at all levels are considered when planning counter-mobility tasks. Barriers should be planned to achieve the desired effect on the enemy either to disrupt, turn, fix or block him. They may be terrain, target or situation oriented.

MAIN ENGINEER COUNTER-MOBILITY TASKS

6. Counter-mobility tasks involve the creation of obstacles by, for example laying minefields, demolition and enhancement of natural obstacles. The effectiveness of the obstacle can be increased by combining obstacle types with fire and manoeuvre.

SURVIVABILITY SUPPORT

7. Survivability includes all aspects of protecting personnel, weapons and materiel from enemy weapon and detection systems. It may include deception measures. All arms are responsible for their own survivability. Engineers will augment and enhance unit survivability measures within the limits of available resources and the priorities of the tactical commander. Engineer effort will be concentrated on tasks requiring special skills or equipment. Survivability measures begin with the use of all available concealment and natural cover, followed by digging and constructing fighting and protection positions. As time and the tactical situation permit, these positions may be improved.

MAIN ENGINEER SURVIVABILITY TASKS

8. The main engineer survivability tasks are:

a. Assistance in the preparation and construction of field fortifications.

b. Hardening and construction of protective works, including collective protection against NBC attack.

c. Assistance with camouflage, concealment and deception.

d. Assistance in the clearance of fields of fire.

e. Advice on the selection of buildings and other elements of the infrastructure for defence and protection.

GENERAL ENGINEER SUPPORT

9. General engineer support involves the provision of engineer advice, technical expertise, resources and work other than the close support provided directly to combat operations. Many of the tasks in this category will be undertaken in the rear areas, although provision

of general engineer support will occur in all areas of the battlefield and in all operations of war.

GENERAL ENGINEER SUPPORT TASKS

10. General engineer support tasks may include the following:
    a. Emergency supply of water.
    b. Construction of air landing facilities.
    c. Airfield damage repair.
    d. Provision and maintenance of utilities and structures.
    e. Maintenance and construction of main supply routes.
    f. Explosive Ordnance Disposal (EOD).
    g. Railways and ports.
    h. Fuel storage and distribution.
    i. Geomatics support.
    j. NBC decontamination.
    k. Emergency supply of energy.
    l. Firefighting.

PRINCIPLES OF EMPLOYMENT

11. **Foresight**. The timely completion of engineer tasks depends on thorough planning based on sound engineer intelligence. It follows that the latter must emanate from the commander's overall intelligence collection plan. Thereafter planning continues in a logical sequence:

    a. The commander states the operational requirement.

    b. The engineer assesses the cost in terms of men, equipment and material, whilst verifying the technical feasibility.

    c. The overall plan is agreed.

    d. The engineer plans in details and executes the work.

12. This sequence will flow smoothly if foresight is used in 4 areas, namely:

a. The procurement of engineer information.

b. The operational planning including the engineer staff from the outset.

c. Early reconnaissance.

d. The ordering of equipment and material.

13. **Priorities of Work**. There are seldom sufficient engineers to carry out all the tasks required of engineers. The engineer must liaise closely with his commander and staff to agree on priorities of engineer work. These must be carefully selected, since subsequent changes leading to re-deployment will reduce the available working time. These priorities must include the provision of an engineer reserve, but due to the likely shortage of engineer units this reserve will often be committed to a low priority task, rather than being allowed to remain idle.

14. **Centralised Control**. The execution of combat engineering tasks requires the judicious deployment and control of men, plant and materials. The most economical and efficient results are normally obtained by centralizing control at the highest practicable level and by the right concentration of effort for each task. By centralizing control the engineer commander can allocate the correct mix of combat engineer, and plant support to the task in hand and can alter this allocation as priorities change and jobs are completed. Consequently the most usual engineer grouping with other arms will be in support and under command for movement rather than directly under command, as this gives the engineers flexibility as situation dictates. Centralized control also makes it possible to constitute an effective reserve of engineers which will be essential in battle.

15. **Cooperation**. Although the principle of centralized control must remain paramount, it is normal for certain engineer units to be affiliated to formations. This means that when these units are moved around the battlefield to deal with high priority task they will be returned to support their affiliated formation whenever it is possible. This principle of affiliation establishes a close degree of cooperation and understanding between engineers and other arms.

TEST QUESTIONS

1. Discuss the main roles of the Combat Engineers?
2. What are the main engineer tasks in the fol:
   a. Mobility Support.
   b. Counter Mobility Support.
   c. Survivability Support.
   d. General Engineer Support.

   Explain the principles of employment of the engineers?

CHAPTER TWO
RESERVED DEMOLITIONS

INTRODUCTION

1. In every land operation, much premium is given to demolition either in the advance or withdrawal. Demolitions are normally prepared and blown by sappers. However, the control of what is to be destroyed, and when, is entirely the responsibility of a supported commander and his staff.

OBJECTIVES

2. On the completion of this Chapter, officers should:

a. **Know.**

(1) Types of Demolition.

(2) Duties of the following:

(a) Guard Commander.

(b) Firing Party Commander.

(3) The documentation.

(4) The importance associated with control points.

b. **Understand.**

(1) The Command and staff responsibilities.

(2) The defence of a reserved demolition.

(3) The withdrawal of the demolition guard.

DEMOLITION

3. Under the general classification, demolition includes the destruction of bridges of all kinds such as:

a. Fixed span bridges over water obstacles.

b. Railway bridges of all types.
c. Viaducts.
d. Military equipment bridges in use by own troops.

4. The term also includes, for the purpose of this module:
a. The closing of lanes in minefields.
b. Cratering of roads and defiles.
c. The blocking of approaches by felling trees or blowing in the side of cutting or by destroying buildings.
d. The destruction of causeways or fords.
e. The destruction of ferries - military or civilian.
f. Inundation by blowing dams, flood gates, canal banks etc.

TYPES OF DEMOLITION

5. **Preliminary Demolition**. Preliminary demolitions are those that do not interfere with our planned tactical movement. Normally, the Commander will delegate authority to fire these demolitions to the engineers as soon as there is no danger of prejudicing surprise or otherwise affecting operations. The earlier preliminary demolitions are fired the better, in order to release engineers for other tasks.

6. **Reserved Demolition**. Reserved demolitions play a vital part in the tactical or strategic plan. The overall commander will control these demolitions and, he is responsible for ordering the firing. Reserved demolitions pose 3 main problems :

a. **Site must be open to Traffic until Fired**. This may mean that simple and quick demolition techniques cannot be used. Rapid Demolition Device (RDD), crates containing large quantity of slap explosive cannot be kept in position across a bridge, nor can all methods of road cratering be adopted

unless special method of protecting the means of firing are used.

b. **Time and Effort in Preparation**. Every reserved demolition must be prepared as a longstanding demolition, able to withstand the effects of weather and traffic vibrations for some time. There must be no possibility of failure; so duplicated firing circuits have to be used. These refinements require more time and effort. Because of maintenance problems and non-productiveness of engineer effort committed on such demolitions that will not be available for other tasks, an engineer regiment should undertake very few reserved demolitions; usually not more than 4.

c. **Firing Parties**. From the time a reserved demolition is prepared, it absorbs a firing party doing no other engineer work. Too many reserved demolitions are bound to tie down engineer troops, which would affect other engineer tasks.

RESERVED DEMOLITIONS PARTIES

7. **Authorized Commander**. The officer empowered to authorize the firing of a reserved demolition is called the authorized commander. As the withdrawal proceeds, authority may be delegated to a lower commander who then becomes the authorized commanders.

8. **Demolition Guard**. A demolition guard is a locally positioned force whose task is to ensure that the site of a demolition is not captured by the enemy before it is successfully fired.

9. **Demolition Firing Party**. The demolition firing party is technically responsible for the demolition. It is normally an engineer party and is often commanded by a junior NCO.

TECHNICAL DEFINITIONS

10. **Uncharged.** A demolition target which has been prepared to receive charges, and the latter being packaged and stored in a safe place.

11. **Charged**. A demolition in which all charges have been placed and which is at one of the states of readiness below:

a. **State of Readiness "1" (SAFE).** The demolition charge has been placed and secured. The vertical and horizontal ring mains are disconnected and the detonators are not inserted in the 2 initiating sets.

b. **State of Readiness "2" (ARMED).** Demolition is ready for immediate firing. The danger of premature firing caused by the close explosion of a bomb or shell when the demolition is armed must be balanced against the time required to bring the demolition from state of readiness "1" (SAFE) to "2" (ARMED). This time will vary with the complexity of the demolition and engineer advice must be obtained. It could take as much as 20 minutes on a large bridge.

12. **Completion**. It is wrong to consider that the firing of a demolition is necessarily the same as completion. Engineers may well require some time after the firing to ensure that the demolition is effective. Time to complete can only be assessed by the men who designed the demolition and will vary in every case. For a major road bridge over a deep water obstacle, the outing of a main span may well complete the demolition. However, in the case of closing a minefield lane (which may involve cratering); it may often be necessary to scatter antitank and anti-personnel mines after the craters have been blown. It will be necessary in this case for

engineers to continue to be protected by the demolition guard until completion. In the event of a misfire or only partial destruction, the demolition guard must clearly continue to provide protection while the charges are reset or additional charges placed on the demolition.

COMMAND RESPONSIBILITIES

13. **The Authorized Commander**. Initially, the authorized commander will be the formation commander responsible for the operational plan and he:

a. Classifies a demolition as reserved.

b. Orders a formation or unit to provide a demolition guard.

c. Orders whether or not the demolition should be fired on the initiative of the commander on the spot in case of imminent capture.

d. Orders changes, as necessary, in the state of readiness.

e. Orders the demolition to be fired.

At any stage, before or during the operation, the authorized commander may delegate these responsibilities. For example, when one formation withdraws through another which is holding an intermediate position; it is normal for control to pass to the commander of the holding formation who then becomes the authorized commander. Delegation of control is an important command decision.

14. **The Engineer Commander**. The Engineer Commander does the fol:

a. Advises the formation commander on the technical factors, including engineer effort available, affecting his

choice of reserved demolitions.

b. Orders the preparation of the demolition.

c. Provides the demolition firing party.

d. Initiates the instructions for the commander of the demolition firing party on AF W4012B (Annex A).

15. **The Demolition Guard Commander**. He receives his initial orders on AF W4012C (Annex B) and thereafter:

a. Commands all troops at the demolition site including the demolition firing party.

b. Ensures the safety of the demolition from enemy attack or sabotage.

c. Controls traffic and refugees.

d. Passes to the commander of the demolition firing party orders in writing on the AF W4012B to change the state of readiness, and in most circumstances to fire the demolition.

e. Keeps the authorized commander informed of the state of preparation of the demolition and the operational situation at the demolition site.

f. After the demolition, he reports to the authorized commander on its effectiveness.

16. **Demolition Firing Party Commander**. He is an engineer personnel who:

a. Maintains the state of readiness ordered.

b. Fires the demolition when ordered and ensures it is successful.

c. Reports the result of the demolition.

COMMUNICATIONS

17. The authorized commander must ensure that there is a clear cut channel whereby he can pass orders to the commander of the demolition firing party to change the state of readiness and to fire the demolition. This channel will normally be through the demolition guard commander, whose command includes the firing party, and must be known and understood by all concerned. To ensure success, a combination of methods will often be used among which include:

a. **Normal Command Channels**. With several links involved this may lead to delay, but it has the advantage that many of those concerned are automatically kept in the picture.

b. **A LO with a Radio Set**. This is often valuable as the demolition guard commander can then devote himself to his other duties in the immediate vicinity of the target.

c. **Pool Radio**. A pool radio set allotted to the demolition guard commander, either on the appropriate command net or on a special net.

d. **Engineer Net**. There should be provision for an engineer net.

e. **Arty Communication**. Artillery communications to an OP with the demolition guard commander.

f. **Orders**. The orders may be given personally on the spot by the authorized commander.

STAFF RESPONSIBILITIES

18. The staff must ensure that:

a. The formation commander's orders as in Paragraph (13a - e) reach all concerned. This is best done in the form of an annex to an operation order. Orders

concerning preliminary demolitions can also be given in this form. They should make clear what routes or areas are closed to traffic and from what time.

b. Any special communications required to pass the formation commander's orders to change states of readiness and to fire, are set up.

c. Demolition Guard Commanders are issued with written orders on AF W4012C; see Paragraph 19c below.

19. **AFW 4012C - Orders to the Demolition Guard Commander**. This proforma is self-explanatory but the following points should be particularly noted:

a. The form can be completed from the information in the suggested annex to the operation orders, so that it needs not necessarily be completed by the headquarters issuing the operation order. It is the responsibility of the staff to issue this form, not the engineers.

b. "Code sign" should be interpreted as "nickname". This is for easy reference to the location, e.g. "RABBIT TABLE 675892". This must not be confused with a code word, used to give an executive order.

c. The authorized commander must therefore make up his mind whether the demolition guard commander should be allowed to fire on his own initiative in a real emergency or not.

d. The delegation of authority to fire should be passed to the demolition guard commander and the new authorized commander using this code word and the address group or encoded title of the new authorized commander. An effective time can be added in code if required.

e. Every potentially authorized commander must have a copy of the AFW 4012C. When authority is to be delegated to

an unforeseen commander, the current authorized commander must pass his own copy of AFW 4012C to the new authorized commander.

20. **AFW 4012B - Orders to the Commander**

Demolition Firing Party. It caters for several possibilities:

a. Preliminary demolition (Paragraphs 4(a) or 4(b).

b. A reserved demolition with a demolition guard paragraph 4(d).

c. A reserved demolition with no demolition guard (Paragraph 4 (c) or 4(d). Paragraph 5 is the equivalent of Paragraph 14 on AFW4012C and must in this case, be completed. In this situation, the staff are of course, responsible for ensuring that AF W4012B is correctly completed in accordance with the Commander's orders for the reserved demolition.

21. **Modification for Road Denial Bands**. The final withdrawal routes through a road denial band may contain a large number of minor demolitions and it will be normal for the demolitions on one route to be grouped under one set of orders. The authorized commander will finally be the battalion or company commander of the covering troops withdrawing on the route.

PLANNING TIMES

22. The time and labour needed to prepare a demolition will vary from 2 section hours for a group of craters to one troop day for a 1,000 foot bridge. In an emergency, demolitions may be carried out much more quickly by using Rapid Demolition Devices. It must be appreciated, however, that much more explosive is required.

FIRING PROCEDURE

23. **Changing States of Readiness**. On arrival at the reserved demolition, the demolition guard commander must find out how long it takes to change the state of readiness of the demolition and how long it takes to complete the demolition after firing e.g. nuisance mining of the area. This information must be passed to the authorized commander. He must also check on his means of communication in Paragraph 4 of AFW 4012C (Annex B to Part 1). On receipt of the order to change the state of readiness of the demolition, the guard commander will fill in Paragraph 8 of his form and Paragraph 3 of the firing party commander's AFW 4012B (Annex G to Part 1). He will then report the change of state of readiness of the demolition as stated in Paragraph 9 of his instructions.

24. **Changes in Authorized Commander**. The guard commander must pay particular attention to the instructions in Paragraphs 14 and 16 and to the relevant code words in Part V of the AFW 4012C.

25. **Orders to Fire**. On receipt of the order to fire the demolition, the guard commander will pass it to the commander of the demolition firing party and fill in Part IV of AFW 4012B.

26. **Misfire Drill**. Should the electrical circuit be broken, the demolition guard commander must allow time for the firing party commander to go forward and initiate the firing of the demolition by means of the safety fuse initiation set.

27. **Inspection and Reporting**. The firing party commander must inspect the demolition after it has been fired and report the results on the engineer net and then return the completed form

(AFW 4012B) as detailed in Paragraph 13. The demolition guard commander must also report the results immediately to the authorized commander.

28. **Security**. The codeword in Part V of the guard commander's instructions must be carefully noted.

SUMMARY

29. The successful firing of the reserved demolition will depend largely on the skill of the defence of the demolition. Plans must be made to cover all foreseeable contingencies and the withdrawal of units through the demolition requires careful co-ordination.

TEST QUESTIONS

30. Write out the answers to the following questions based on this chapter:

a. What are the types of demolition?
b. Define a reserved demolition?
c. What is a Demolition Guard?
d. What does 'charged' and 'uncharged' mean?
e. What is Demolition Firing Party?
f. Who is the Authorized Commander?
g. What are the responsibilities of the Authorized Commander?

Annexes:

A. AFW 4012B.
B. AFW 4012C.

ANNEX A TO
CHAPTER 2

Army Form W 4012 B
R.N. Form S 1543
(Revised 1968)

Serial No.....
Security Classification.....

ORDERS TO THE DEMOLITION FIRING PARTY COMMANDER

NOTE: Parts I, II and III will be completed and signed before this card is handed to the Demolition Firing Party Commander. Para 4 and 5 can only be altered by the authority issuing these orders. In such cases a new form will be issued and the old one destroyed.

From.....
To.....

Part I: Orders for Preparing and Charging the Demolition Target

1. a. Description:.....
   b. Location:.....
   Map Name and Scale.....
   Sheet No.....Grid Reference.....
   c. Code word of Demolition Target (if any).....
   d. Attached photographs and special technical instructions.....
   .....

2. The DEMOLITION GUARD is being provided by (Unit).....

3. You will prepare and charge the demolition target to the STATE OF READINESS by..... hours on..... (Date).....

Any changes may only be made on the order of the issuing authority, or by the officer designated in Para 4d and will be recorded below.

Note: All orders received by message will be verified by the code word at Para 1c. If the order is transmitted by an officer in person, his signature and designation will be obtained in the column headed "Authority".

Security Classification.....

PART II -ORDERS FOR FIRING

Note: The officer issuing these orders will strike out the sub-paras or paras 4 and 5 which are not applicable. When there is a Demolition Guard, subpara 4d will always be used, and para 5 will always be struck out.

4. a. You will fire the demolition as soon as you have prepared it.

b. You will fire the demolition at ..... hour on..... (date).....

c. You will fire the demolition on receipt of the code word.....

d. You will fire the demolition when the officer whose designation is .....has signed para. 8 below.

Emergency Firing Orders (ONLY applicable when there is No Demolition Guard)

5. YOU WILL NOT FIRE the demolition in any circumstances except as ordered in para.4 above or YOU WILL, FIRE the demolition on your own initiative if the enemy is in the act of capturing it.

PART III -ORDERS FOR REPORTING

6. After firing the demolition you will immediately report results to the officer who ordered you to fire. In the event of a partial failure, you will warn him, and immediately carry out the work necessary to complete the demolition.

7. Finally you will immediately report the results to your Unit Commanding Officer (See Para l3).
Signature of Officer issuing these Orders.....
Name (in capitals).....
Designation.....
Time of issue .....
Date of issue.....

PART IV-ORDER TO FIRE

8. Being empowered to do so I order you to fire NOW the demolition described in Para 1.
Signature.....
Name (in capitals).....
Designation.....
Time.....

READ THESE INSTRUCTIONS CAREFULLY
PART V -GENERAL INSTRUCTIONS

9. You are in technical charge of the preparation, charging and firing of the demolition target described. You will nominate your deputy forthwith, and compile a seniority roster of your party. You will ensure that each man knows his place in the roster, understands these instructions, and knows where to find this form if you are hit or unavoidably absent. You will consult with the Demolition Guard Commander on the sitting of the firing point.

10. You must understand that the DEMOLITION GUARD Commander (where there is one) is responsible for:

a. Operational command of ALL troops, at the demolition site.
(You are therefore under his command). b. Controlling all traffic and refugees.

c. Giving you the order to change the STATE OF READINESS from "1 (SAFE)" to "2(ARMED)" or back to "1 (SAFE)" again. You will inform him of the time required for such a change.

d. Passing to yell the actual order to fire.

11. When there is no demolition guard and you are instructed in Para 4 to accept the order to fire from some particular officer it is important that you are able to identify him.

12. If you get orders to fire other than those laid down in Para 4 you should refer them to the Demolition Guard Commander or if there is no Demolition Guard Commander, to your immediate superior. If you cannot do this, you will ONLY depart from your written instructions when you are satisfied as to the identity and

over-riding authority of whoever gives you these new orders, and you will get his signature in Para 8 whenever possible.

13. The report to your Unit Commanding Officer, as called for in Para 7, should contain the following information (where applicable):

a. Identification reference of demolition.
b. Map reference.
c. Time and date when demolition was fired.
d. Extent of damage accomplished, including:
    (1) Estimated width of gap.
    (2) Number of spans down (in the case of a bridge).
    (3) Size and location of craters in a road or runway.
    (4) Mine laid.
e. Sketch showing effect of demolition

ANNEX B TO
CHAPTER 2

ARMY FORM W4012C (Revised 1971)

Serial No.....Security Classification.....

ORDER TO DEMOLITION GUARD COMMANDER

Notes: .....

1. This form will be completed and signed before it is handed to the Commander of the Demolition Guard.

2. In completing the form, all spaces must either be filled in or lined out.

3. The officer empowered to order the firing of the demolition is referred to throughout as the "Authorized Commander"

From.....

To.....

PART 1 -PRELIMINARY INSTRUCTIONS

1. a. Description of target.....

   b. Location:.....

   Map Name and Scale.....Sheet No..... Grid Reference.....

   c. Code word or code sign (if any) of demolition target..... .....

2. The authorized Commander is..... (give appointment only). If this officer should delegate his authority you will be notified by one of the methods shown in Paragraph 4, below.

3. **THE DEMOLITION FIRING PARTY COMMANDER** has been/will be provided by .....

4. All messages, including any code words or code signs (if any) used in these orders, will be passed to you by:

a. Normal command wireless net, or

b. special liaison officer with communications direct to the authorized commander, or

c. Telephone by the Authorized Commander, or

d. The authorized Commander personally, or

e. .....

(Delete those NOT applicable)

Note: All orders sent by message will be prefixed by the code word or code sign (if any) at paragraph 1c and ALL such messages must be acknowledged.

PART II - CHANGING STATES OF READINESS

5. The demolition will be prepared initially to the State of Readiness by ..... hours on..... (date).

6. On arrival at the demolition site, you will ascertain from the Commander of the Demolition Firing Party the estimated time required to change from State "1 (SAFE) to State "2 (ARMED). You will ensure that this information is passed to the Authorized Commander and is acknowledged.

7. Changes in the State of Readiness from state "2" (SAFE) to Sate "2" (ARMED) or from State "2" to State "1" will be made only when so ordered by the Authorized Commander. However, the

demolition may be ARMED in order to accomplish emergency firing when you are authorized to fire it on your own initiative.

8. A record of the changes in the State of Readiness will be entered by you in the table below, and on the firing orders in possession of the Commander of the Demolition Firing Party.

Note: If the order is transmitted by an officer in person, his signature and designation will be obtained in the column headed "Authority".

9. You will report completion of all changes in the State of Readiness to the Authorized Commander by the quickest means.

PART III - ORDERS FOR FIRING THE DEMOLITION

10. The order for firing the demolition will be passed to you by the Authorized Commander.

11. On receipt of this order you will immediately pass it to the Commander of the Demolition Firing Party on his demolition order form ("Orders to the Demolition Firing Party Commander").

12. After the demolition has been fired you will report the results immediately to the Authorized Commander.

13. In the event of a misfire or only partially successful demolition you will give the firing party protection until such times as it has completed the demolition and report again after it has been completed.

Notes: 1. One sub-paragraph of paragraph 14 must be

deleted.

2. The order given herein can only be altered by the issue of a new form, or in emergency by the appropriate order (or code word if used) in Part V.

14. a. You will order the firing of the demolition only on the order of the Authorized Commander or

b. If the enemy is in act of capturing the target you will order the firing of the demolition on your own initiative.

PART IV - CODE WORDS (IF USED)

Action to be taken:.....

a. Change State of Readiness from "1" to "2" (See Paragraph 7).

b. Change State of Readiness from "2" to "1" (See Paragraph 7).

c. Fire the demolition (See Paragraph 10).

d. Paragraph 14a is now cancelled. You are now authorized to fire the demolition if the enemy is in the act of capturing it.

e. Paragraph 14b is now cancelled. You will order the firing of the demolition only upon the order of the Authorized Commander.

f. Special authentication instructions, if any.

g. The Authorized Commander is changed to.....

The new Authorized Commander can be indicated by his address group or encoded title. An effective time can be added in code if required. PART V

Signature of officer issuing these orders.....

Name (printed in capital letters).....
Rank.....Appointment .....
Time of issue.....hours . . . . (date)

CHAPTER THREE
RIVER AND GAP CROSSING OPERATIONS

INTRODUCTION

1. This Chapter should be studied in conjunction with Chapter 1. The first part of the Chapter deals with the roles and responsibilities of the engineers. This chapter is aimed at highlighting the various engineer assistance during an oppose river crossing operations.

OBJECTIVES

2. Officers on completion of this Chapter will cover the spectrum of obstacles and will:

a. **Know**.

(1) Phases of a crossing operation.
(2) Possible variations in crossing operations.
(3) Characteristics of Engr with crossing obstacles before planning a crossing operation.

b. **Understand**.

(1) The command and control of obstacle crossing.
(2) The importance of careful assessment of obstacles before planning a crossing operation.

PHASES OF RIVER CROSSING

3. A crossing operation should include the following phases:
a. **Reconnaissance**. To plan the river crossing, a commander will require:
(1) **Combat Intelligence**. Combat

Intelligence is an understanding of the way in which the enemy can affect the operation. This he will gain from the combat intelligence provided in the normal way by his intelligence staff.

(2) **Engineer Intelligence**. Information on the crossing site and bank conditions can be obtained by reconnaissance from boats or amphibians. Where units are in contact with the enemy, surface swimmers and shallow water divers can be used. The equipment which they require for their task include gap measuring devices, clinometers for measuring bank slopes, instruments for measuring the depth and current of the river and for examining the river bottom. The location of enemy mines laid either on the banks or in the water, should be one of the important questions to be answered by the technical reconnaissance. Alternative sites for both swimming and fording crossing should always be reconnoitred.

b. **Assault**. An infantry assault in boats, probably at night, to establish a bridgehead of sufficient size to allow bridging, rafting, swimming or fording to take place.

c. **Build Up**. This may include:

(1) Swimming of amphibious vehicles.

(2) Opening of bridges or rafts to pass tanks and other vehicles into the bridgehead. Current river crossing equipment is shown at Annex A.

d. **Consolidation**. This includes the establishment of a coherent bridgehead defence against counter attack and the expansion of the bridgehead into a firm base from which to break out.

e. **The Break Out.** The technical problems associated

with the crossing of large water obstacles are:

(1) Getting men across (the Assault Phase).

(2) Getting swimming vehicles across (Amphibious Follow up).

(3) Getting non-swimming vehicles across (Assisted Follow up).

ASSAULT PHASE

4. This task will fall primarily on the infantry. Planning will have to take account of the following:

a. The allocation and security of assembly area and boat off- loading points. The latter should be as far forward as possible, ideally in the FUP.

b. The carrying or towing of boats to the river.

c. The importance of allowing time in the planning for these detailed infantry tasks, especially if the operation is at night.

5. The infantry will be supported by direct and indirect fire from the home bank provided by other infantry units, armour and artillery. An initial assault by infantry in APCs is tactically difficult as it is unlikely that the APCs will be able to exit in any semblance of a tactical formation. In all but a complete unopposed crossing therefore, the first waves of assaulting infantry must be ferried over the river in assault boats, using either paddles for a silent crossing or outboard motors. The ferrying must be done by soldiers not committed to the assault just like a number of other tasks for the operations. A bank group is formed for these purposes.

AMPHIBIOUS FOLLOW-UP

6. It is likely that some of the follow up echelon will cross the

river by swimming their vehicles. A strong bridgehead will be required against counter attack.

ASSISTED FOLLOW-UP

7. This section concerns resources not normally under battalion command. In order to avoid delay on reaching a water obstacle, commanders and staff must plan ahead to ensure that bridging is grouped with appropriate formations and units, resources of men and material are available when required and suitable harbour areas and routes are allocated for engineer units and equipment.

8. The bridge and rafting sites should be within the bridgehead seized by the initial assault so that work can start on them as soon as possible. Ideally, construction should start at night to achieve a measure of protection. The selection of the site for crossing should be such that the chances of its discovery by the enemy are reduced to the minimum.

ENGINEER ASSISTANCE

9. There will be a considerable demand for engineer assistance in a crossing operation apart from the work involved in the construction and operation of bridges and rafts. The requirement is likely to fall under the following:

a. **Reconnaissance**. Parties using boats, surface swimmers or shallow water divers can cover the water gap and conventional reconnaissance parties, the home and far banks.

b. **Improvements to Crossing Sites**. This can be:

(1) Work on the approaches to improve the going.

(2) Alteration in the bank profile to ease the problems of entry and exiting.

(3) The clearing of mines on the banks and underwater.

(4) Removal of underwater obstructions.

(5) Laying of track ways on the banks and underwater.

(6) Improvements to the going.

c. **Assistance to Exiting Vehicles**. This assistance can be by winching from pathfinder vehicles or from another vehicle that has already exited. Ground anchors can be placed on the far bank by troops, or by rocket, and then used by vehicles to winch themselves out. Fixed lines can be used to improve the rate of ferrying and to ensure exiting at the same place, where track way may be laid down.

d. **Assistance to Vehicles in Difficulty**. This assistance includes recovery of vehicles that may have drowned, broken down or drifted away out of control.

COMMAND AND CONTROL

10. **General**. The movement of bridging equipment, troops, tanks and vehicles through assembly areas, over the river, and their dispersal on the far side must be strictly controlled. The control headquarters must make the best use of the resources available and provide a flexible organization able to react quickly to any changes in the tactical situation and the means of crossing.

11. **Basic Requirement for Control**. These include:

a. **Clear Orders**. These should state:

(1) Who authorizes the engineers to start work on the construction of bridges and rafts.

(2) Who authorizes the start of the amphibious crossing and site preparations.

(3) The level at which the use of boats, rafts and bridges is to be controlled in each phase of the crossing.

(4) Who controls the traffic to and over the various crossing sites.

b. **Bank Group Organization**. This is normally provided by a company from a battalion not committed to the assault. The tasks of the bank group are:

(1) Clearance of the home bank, if this has not been done already and security of the FUP.

(2) Organization of the Boat Off-loading Point, where the assault boats are taken off their transport. This should be as far forward as possible.

(3) Control of the movement forward of the assaulting infantry.

(4) Manning the assault boats and ferrying, in particular returning empty boats to the home bank for succeeding waves.

(5) Construction in conjunction with assault pioneers of infantry rafts, if these are to be used.

(6) Providing fire support from the home bank.

12. Tank battalion and Recce battalions may also be able to provide the following assistance:

a. Traffic control using their excellent communications.

b. Surveillance of the far bank.

c. Elimination of enemy direct fire weapons immediately before or during the assault.

d. Destruction of enemy on the approach routes to the site and on the objective.

e. Where suitable viewpoints exist ATGW may be of particular value in providing anti-tank defence of the bridgehead. Their longer ranges may enable them to engage targets on the enemy approach routes beyond the tanks.

13. In a swim or ford crossing, the battalion carrying out the

operation provides:

a. **A Crossing Controller**. A Crossing Controller is likely to be the battalion 2iC, who is placed well forward near the obstacle to control not only the calling forward of vehicles in their correct order by also actual crossing. He must ensure that each crossing is used to its maximum capacity. As each company group comes forward it provides a LO to the crossing controller as an additional check.

b. **An Entry Bank Master**. An Entry Bank Master directs the entry of each amphibian into the water in the sequence laid down. He will normally require the assistance of guides and be in communication with the Crossing Controller.

c. **An Exit Bank Master**. An Exit Bank Master is assisted by guides and supervises the exiting of the amphibians. He also coordinates the recovery and dispersion from the exit sites. He must cross the river by assault boat or in the leading vehicle and have communications to the Crossing Controller.

d. **Traffic Control**. A comprehensive traffic control organization must be set up by the senior headquarters controlling the crossing. Depending on the level of operation, this may be based on elements of a reconnaissance regiment, provost and unit reconnaissance troops or platoons. Traffic control headquarters should be set up alongside the operations cell. This organization is required to enable serials to be switched between crossing sites and to prevent bunching at the crossing site and on the routes to them. Control is based on a series of traffic posts and waiting areas, with signed lateral and forward routes. The traffic organization requires its own communication, recovery

facilities deployed along the routes and medical support at crossing sites. At bridging and rafting sites, close liaison must be maintained with engineer commanders to report on progress and delays. The control organization must ensure that vehicles are available at crossing sites as soon as the bridge or rafts are ready. This may mean ensuring alternative crossing places are available and amphibious bridging and ferries are switched between sites to avoid enemy interference, if this is not done the traffic control problem will be aggravated. If this switching is to be a timed programme, the traffic plan and vehicle priority tables can be written to allow for it. Additional waiting areas may be needed close to the river to ensure that the bridge or raft is never kept waiting for crossing vehicles.

VEHICLE PRIORITY TABLES

14. Crossing formations and units must prepare Vehicle Priority Tables. The following must be borne in mind:

a. Every formation and unit involved in the early stages of the crossing must prepare a detailed vehicle priority table, arranged in the load classes of the ferries and bridges to be built. Similar tables will be necessary when considerable numbers of amphibious vehicles are compelled to use a limited number of crossing sites. The aim is to ensure that transport requirements are significantly reduced. Nevertheless, work is bound to take an hour or more and cannot take place under fire without excessive casualties. There is therefore a need for a bridgehead to be formed and for far bank clearance exactly as for a river crossing. Both the staff and the traffic control organization can refer to it and avoid confusion.

b. In the initial stages, there is normally a restriction on the number of vehicles, which units may take into the bridgehead. This is due to the restricted space, the limited capacity of the ferries and bridges and the need to deceive the enemy as to the size of the build up. However, units must always work out a priority table for all their vehicles, so that when more are allowed into the bridgehead there is no confusion.

POSSIBLE VARIATIONS

15. The crossing of water obstacles may not always be as part of an advance or assault. A withdrawing force may be required to use river or gap crossing equipment to extricate itself in the face of the enemy. The technical problems do not change, but staff work and organization must be particularly good so that full advantage is taken of the inherent flexibility of the equipment. In particular, the following points must be covered:

a. Routes to and away from the sites must be reconnoitred, signed and promulgated. Waiting areas must be established. Traffic control must be organized.

b. Troops must be allocated to protect the bridge during construction and until the crossing has been completed.

c. Emergency demolition or denial of the equipment must be considered and the normal AFW 4012B and C procedures implemented. (i.e. Reserved Demolitions).

d. Liaison Officers will be required at the bridge sites to ensure the smooth passage of units to the rear.

e. Air defence may have to be established very quickly.

f. Recovery vehicles will be required to clear the site of any vehicle casualties.

GAP CROSSING

16. In an undulating terrain, gaps features, especially in sizes may vary. The fact that a gap is small does not necessarily mean it is easily fordable. Crossing can even be more difficult especially where gaps with steep banks and fast current are encountered. Similarly, although the act of bridging a gap may be simpler, the enemy threats to the crossing operation as a whole could pose more dangers. Therefore, the planning and organization discussed earlier in this module will often have to be fully carried out. The bridges and rafts are still bottlenecks restricting the building on the far side of the obstacles.

17. Small rivers are often fast-flowing with steep sides. This combination will usually prohibit swimming except occasionally on fixed-line and with prepared exits. Canals also frequently have sides which are too steep for APC to climb.

18. In these circumstances, the attacker is forced to use fixed bridging on expedients such as the following:

a. **Fixed Bridging**. Construction times for the Medium Girder Bridge (MGB) (up to Class 60) and the Air portable Bridge (APB) (up to Class 16) are short and the manpower and transport requirements are very significantly reduced. Nevertheless, work is bound to take an hour or more and cannot take place under fire without excessive casualties. There is therefore the need for a bridgehead to be formed and for far-bank clearance exactly as for a river crossing.

b. **Assault Bridging**. The deployment of tankmounted bridges must be covered by the fire of other tanks, and possibly, by smoke when in the face of the enemy.

c. **Expedients**. These include fascines (either single or paired), hardcore and the use of tank dozer blades. If water is flowing in a gap, care must be taken not to block the stream by such expedients or flooding will occur.

SUMMARY

19. Given the right conditions, the combination of amphibious vehicles and bridges enables a river crossing to be made far faster and with greater choice of crossing sites than ever before. In particular, the attacker has now to rely less on tracks and roads leading to the river. On the other hand, tanks and heavy vehicles will still have to cross deep rivers by bridges or ferries. A river crossing operation requires careful preparation and planning, detailed reconnaissance, good control, a rapid build up and bridgehead large enough to contain the necessary troops to repel any counter attack.

Annex:

A. Details of River Crossing Equipment.

TEST QUESTIONS

20. Answer the following questions based on this Chapter:

a. What are the 5 phases of a crossing operation?

b. What are the tactical problems associated with the crossing of a large water obstacle?

c. What will you take into account when planning the assault phase of a river crossing?

d. Requirement for engineer assistance is likely to fall under four headings; what are they?

e. What is Bank Group Organization?

f. Who is an Entry Bank master?

g. Who is an Exit Bank Master?

I. What are the forms of improvements to a crossing site?

CHAPTER FOUR
BRIDGING

INTRODUCTION

1. The success of any advancing force, especially the maneuver elements, solidly depends on the mobility skills of combat engineers. During advance, it is the sole responsibility of the engineers to improve and maintain Main Supply Routes (MSR) and bridge gaps and obstacles. These tasks are carried out both in forward and rear areas of operation.

2. In carrying out some of these engineer mobility tasks, various types of bridges in the NAE inventory can be deployed. Assault bridges in the forward areas and communication bridges at the rear. This is to help the maneuver force quickly cross both wet and dry gaps in order to enable them maintain the momentum of the advance, and to ensure that all loads and equipment irrespective of their weight, are carried across the gaps.

OBJECTIVES

3. On the completion of this chapter, officers should:

a. **Know**.

(1) Types of bridges:
  (a) Military bridges.
  (b) Non-military bridges.

(2) Types of assault and communication bridges.

(3) Characteristics of assault and communication bridges.

(4) Configuration of Compact Bailey Bridge (CBB).

(5) Importance of bridges.

(6) Various terms and abbreviations used in bridging.

(7) Understand the types of bridges for both assault and communication purposes.

TYPES OF BRIDGES

4. **Military Bridges**. These are temporary bridging structures. Military bridges are used to span gaps for military purposes and use only, and when no longer needed, they are retrieved and transferred to other desired location.

5. **Non Military Bridges.** These are permanent bridging structures over a gap.

TYPES OF MILITARY BRIDGES

6. Military bridges are usually described as:
   a. Fixed bridges.
   b. Floating bridges.
   c. Non-equipment bridges (NEB).

7. Military bridges can broadly be classified as communication bridges and assault bridges. This classification largely depends on the functions they carry out in the field. Communication bridges are used mainly at the rear for supply, while assault bridges are used mostly in forward areas during operations.

TYPES OF ASSAULT AND COMMUNICATION BRIDGES

8. **Assault Bridges**. Examples of assault bridges are:
   a. MGB – Medium Girder Bridge.
   b. APB – Air Portable Bridge.
   c. AVLB – Armour Vehicle Launch Bridge.
   d. FFB – Foldable Float Bridge.
   e. PBS – Pontoon Bridge System.

9. **Communication Bridges**. Examples of communication bridges are:
   a. BB – Bailey Bridge.
   b. CBB – Compact Bailey Bridge.

c. APB Raft – Air Portable Bridge Raft.
d. NEB – Non Equipment Bridge.

CHARACTERISTICS OF ASSAULT AND COMMUNICATION BRIDGES

10. **Assault bridges.** The following are the characteristics of assault bridges:

a. They are lightweight bridges.
b. They are easy to assemble.
c. They are hand-built bridges.
d. They have short time of construction.
e. They require small assembly party.
f. They are used to play more than one role in assault operation.
g. Most often, they are used for bridging narrow gaps.
h. They are highly mobile and versatile.
i. They can be easily launched and de-launched.

11. **Communication bridges.** The following are the characteristics of communication bridges:

a. They are heavyweight bridges.
b. They offer different types of construction configuration.
c. They are used to span gaps at the rear as communication bridges.
d. They require large assembly party.
e. They take longer time to construct.
f. They are more difficult to be launched and delaunched.
g. They are mostly used for bridging broader gaps.

CONFIGURATION OF COMPACT BAILEY BRIDGE (CBB)

12. Compact bailey bridge offers the following types of construction configurations:

a. **SS** – Single Truss, Single Storey Unreinforced.

b. **SSR** – Single Truss, Single Storey Reinforced with Standard Chords.

c. **SSRH** – Single Truss, Single Storey Reinforced with Heavy Reinforcement Chord.

d. **DS** – Double Truss, Single Storey Unreinforced.

e. **DSR1** – Double Truss, Single Storey Reinforced with Standard Reinforcement Chord.

f. **DSR1H** – Double Truss, Single Storey Reinforced Inner truss with Heavy Reinforcement Chord.

g. **DSR2** – Double truss, Single Storey Reinforced Inner and Outer truss with Standard Chords.

h. **DSR2H** - Double truss, Single Storey Reinforced Inner and Outer truss with Heavy Reinforcement Chord.

i. **DD** – Double Truss, Double Storey Unreinforced.

j. **DDR1** – Double Truss, Double Storey Reinforced Inner truss with Standard Reinforcement Chord.

k. **DDR1H** – Double Truss, Double Storey Reinforced Inner truss with Heavy Reinforcement Chord.

l. **DDR2** – Double Truss, Double Storey Reinforced Inner and Outer truss with Standard Chords.

m. **DDR2H** – Double Truss, Double Storey Reinforced Inner and Outer truss with Heavy Reinforcement Chords.

IMPORTANCE OF BRIDGES

13. In modern warfare, bridges are regarded as indispensible weapons used:

a. To fight gap obstacles by creating a way across them.

b. To maintain quick mobility of tanks and equipment across gaps.

c. To ensure safety across gaps.

d. To give confidence to troops and drivers crossing gap obstacles.

VARIOUS TERMS AND ABBREVIATION USED IN BRIDGING

14. The following are terms used in bridge construction:

a. **AR SPAN** – the distance between the angle of repose pegs on home and far banks.

b. **BAYS** – 1.8m (6ft) panel length.

c. **LAUNCH** – The stage of pushing forward the bridge which gets the nose on to the far bank.

d. **BOOM** – All other movements of the bridge during construction.

e. **CONFIGURATION** – The way components are carried on the 12 pallets.

f. **BSB** – Bank Seat Beam.

g. **RR** – Rocking Rollers.

h. **LNL** – Launching Nose Light.

i. **LNH** – Launching Nose Heavy.

j. **n** – Number of bays in bridge.

k. **N** – Nose Tip Height.

l. **O** – Position of Rear End of Bridge.

m. **DS** – Double Storey.

n. **SS** – Single Storey.

o. **SJP** – Span Junction Post.

p. **SJB** – Span Junction Bay.

q. **AR** – Angle of Repose.

TEST QUESTIONS

15. Write out the answers to the following questions based on this chapter:

a. What are the characteristics of Assault Bridges?

b. List the importance of bridges in military operations.

c. Briefly define the following: (1) Bays. (2) Configuration. (3) Boom. (4) AR Span.

d. Differentiate between assault and communication bridges.

e. List the types of military bridges.

f. What is the meaning of the following? (1) BSB. (2) LNL. (3) LNH. (4) n. (5) N. (6) SJB. (7) SJP.

ANNEX A TO CHAPTER 3

DETAILS OF RIVER CROSSING EQUIPMENT

APPENDICES

1. The Medium Girder Bridge (MGB).
2. The Class 16 Bridge (Air portable) (APB).
3. The MS Amphibious Equipment. (included for interest only).
   The Infantry Assault Boat Raft.

CHAPTER FIVE
IMPROVISED EXPLOSIVE DEVICE AND EXPLOSIVE ORDNANCE AWARENESS AND RECOGNITION

INTRODUCTION

1. Contemporary conflicts have assumed a new dimension in which conventional forces are faced with unconventional tactics used by asymmetric/non-state actors. This has been the case since the end of the Cold War between the Western and Eastern blocks. Thus, conventional forces have made fervent attempts to adjust their doctrines to accommodate asymmetric tactics such as guerilla warfare, terrorism, insurgency, militancy and so on. Asymmetric forces resort to the use of hit and run tactics mainly to meet the challenge of disparity in both human and material resources between them and the conventional forces. They strike in the heart of the military, economic, cultural and political targets using rudimentary improvised weapons to dislocate conventional forces. No target seem unethical for them to attack.

2. In the world over, asymmetric groups have used methods like hijacking, murder, arson, bombings etc; as a means of making statements to powerful countries or organizations. They make use of different kinds of weapons to achieve their objective. However, the most common weapon of choice for the asymmetric groups is the Improvised Explosive Device (IED). This is because of its ability to cause maximum carnage and also spread panic in the populace. An IED is defined as an explosive device that is fabricated in an improvised manner; it incorporates destructive, lethal, noxious, pyrotechnics or incendiary chemicals and it's designed to destroy, incapacitate, harass or distract. IEDs may incorporate military stores,

but they are normally devised from non-military components. The military ordnance used by asymmetric groups for IEDs include but not limited to conventional munitions such as high explosive bomb, mines claymores as well as Unexploded Ordnances (UXOs).

3. This chapter therefore seeks to discuss the components of an IED, its means of initiation and the types and methods of recognising IEDs. Thereafter, it will discuss the reporting procedure, ground sign awareness and the principles of combating the IED threat.

COMPONENTS OF AN IED/EXPLOSIVE ORDNANCE

4. IEDs are relatively simple to make with a little research, time and training. It is easy to source for IED components such as batteries, cell phones and radio transmitters. Detonators and explosives such as C4, semtex and dynamite can be found at construction sites and oil rigs. They may also be stolen, purchased legally or produced locally at home or in a makeshift lab. Other materials like fertilizer, sugar, sand, ammonium nitrate, potassium chlorate amongst others can be easily sourced for. As mentioned earlier, UXOs could also be used to make IEDs in order to make them more potent in terms of explosive power and fragmentation. Every IED manufactured must have 6 basic components for it to function. These include firing switch, arming switch, initiator, power source, main charge and container.

5. **Firing Switch**. The firing switch of an IED is also known as the activator or trigger. The trigger activates the detonator and initiates the explosion sequence. The trigger may sense the target, be activated by the target, be a timed trigger or be operated remotely.

6. **Arming Switch**. The arming switch provides safety to the

perpetrator during manufacture of the IED, during transit, deployment as well as escape from accident.

7. **Initiator**. The initiator is also known as the fuse. The initiation system is the mechanism that initiates the electrical charge to set off the device and includes a switch, initiator (usually consisting of a blasting cap) and power source. IEDs can be initiated by wide variety of methods. These methods include but are not limited to initiation based on command, time and victim activation. The initiating methods for IEDs shall be explained in details later.

8. **Power Source**. The power source is also known as the battery. The power source supplies electricity to the trigger or switch and to the detonator. The power source is the component that waits for command from the initiator to activate the switch. Thus, the power source could be any number of batteries or charged capacitors. In some nonelectric designs, a flame could be used as the power source, as it begins the transfer of energy through the firing system that results in detonation of the main charge.

9. **Main Charge**. The main charge is also known as the explosive. The main charge detonates, producing a high pressure shock or blast wave, and may propel shrapnel, toxic chemicals or fire-starting (incendiary) chemicals. The main charge whose effect is often enhanced by a booster charge can be made of military munitions, which provide ready-made fragmentation, or military and/or commercial explosives such as TNT, ammonium nitrate (agricultural fertiliser) and PE4. Additionally, Home Made Explosives (HMEs) such as reactive/energetic chemicals, flammables and industrial gases can also be used as the main charge in an IED. In addition, IEDs often contain armour penetrating and/or anti-personnel components such as copper rods and shrapnel generating objects such as nails, nuts and bolts to achieve maximum levels of fragmentation. However, in order to reduce the possibility of device

detection, terrorist fighters have started developing IEDs that contain no metal or electronic parts and rely primarily on blast effect to cause damage.

10. **Container**. This is also known as the body which holds the IED component parts together. The container may be designed to force the blast in a specific direction. Casings can consist of almost any type of container from an animal carcass to a cigarette packet or soft drink can. Specific identification features are constantly changing based on the imagination of the bomb maker and available resources.

MEANS OF INITIATING IEDS/EXPLOSIVE ORDNANCES

11. Over the years, various methods of triggering IEDs have been developed all in a bid to ensure success of detonation as well as evade disruption. As with all aspects of IED design, initiation methods are constantly evolving and are limited only by the bomb maker's ingenuity. The common ways of triggering IEDs include command wire, time delay, radio controlled, cell phone, victim operated, infra-red and surgically implanted means.

12. **Command Wire**. Command based initiation, either via hard wire or wireless means, enables the perpetrator to determine the exact moment of detonation. Command initiation is often used against in-transit targets that have established some form of routine movement pattern. It is used as an electrical firing cable that affords the user complete control over the device right up until the moment of initiation.

13. **Time Delay**. Time based IEDs enables the bomber to set off the device at a particular time. This is accomplished by the use of time delay circuits or other improvised means which count down to

the particular time for the explosion to take place.

14. **Radio**. The Radio Controlled IED is another form of command operated system. The device is constructed so that the receiver is connected to an electrical firing circuit and the transmitter operated by the perpetrators at a distance. A signal from the transmitter causes the receiver to trigger a firing pulse that operates the switch which detonates the explosives.

15. **Cell Phone**. The cell phone triggering system is also radio-controlled IED incorporating a modified cell phone that is connected to an electrical firing circuit. Cell phones operate in UHF band in line of sight with base transceiver station. In a common scenario, the receipt of a paging signal by phone is sufficient to initiate the IED firing circuit.

16. **Victim-Operated**. Victim activated devices, as the name implies, are designed to be triggered by the intended victim. They contain various types of anti-handling switches which are actuated or triggered by the victim. They are usually camouflaged and include but not limited to the following:

a. Pull/push switches.
b. Release switches.
c. Pressure switches.
d. Collapsing circuit.
e. Anti-probe.
f. Trip wire.

17. **Surgically Implanted**. These IEDs are surgically implanted into the suicide bombers body. The device is designed to evade detection. They contain no metals so that they could not be detected by X-rays. Surgically implanted IED could also be used on

dead bodies, especially the remains of VIPs. The insurgents will find any way possible to get access to the body and surgically implant IEDs. The reason is that bodies of VIPs are always conveyed to burial sites either by road or by air and usually accompanied by dignitaries. The aim is to cause explosions during the transportation of the body(s) to kill the dignitaries and destroy the vehicle/aircraft.

TYPES OF IEDS/EXPLOSIVE ORDNANCES

18. Asymmetric groups globally have all ingeniously manufactured several types of IEDs based on the intended use. Some IEDs are made to explode in a specific manner in order to make statement by the perpetrators while others could be designed solely for particular targets. Some other IEDs are designed based on the method of delivery to the intended targets. The roles and intended impact depends on where they are situated, their destructive capabilities, and how the explosive device is 'delivered' to the target.

19. **Anti-Armour IED**. The Anti-Armour IED (AAIED) is designed to cause casualty on armoured vehicles. It usually consist of the Radio Controlled (RC) receiver which is a common Radio Controlled IED (RCIED) component. The RC receiver is powered by two 9 volt batteries. These IEDs if concealed or buried can be easily detected using metal detectors operated by a well-trained Counter IED team.

20. **Radio Controlled IED**. The RCIED remains a common device used by terrorists. The device typically employs an electrical blasting cap actuated by a RC receiver (normally the Q-Link vehicle alarm). The power source for the RC receiver is normally provided by 9 volt batteries. The design provides the triggerman with the flexibility to target his intended victim(s) and limit casualties among the local population. The RCIED can be detected using metal

detectors operated by a well-trained Counter IED Team. A frequency jamming device can also be employed to disrupt their means of actuation to enable safe disruption.

21. **Suicide Vehicle-Borne IED**. The Suicide Vehicleborne IED (SVBIED) is another type of IED used by terrorists. The IED container is mostly made of metal cylinders or piping. It also uses the RC receiver powered by 9 volt batteries. This category of IED can be prevented through visual checks by trained security personnel and the installation of frequency jammers at strategic locations.

22. **Improvised Hand Grenades**. Thrown IEDs (improvised hand grenades) are common devices employed by terrorists. Plastic and metal containers such as soda, milk, and deodorant cans are used to hold the explosive compound combined with shrapnel material such as nuts, bolts and ball bearings. Typically, thrown IEDs incorporate a short wick or fuse which is ignited by the user prior to employing the device. The method of preventing the use of this IED is to frustrate the movement of the component materials and also prevent the terrorists from getting within throwing range for such IED's.

23. **Person-Borne IED**. A recent trend of terrorists is to use persons to deliver IEDs to their target. The persons are normally worn with suicide vest containing IEDs and concealed to evade physical detection in order to carry out person-borne IED (PBIED) attacks. Most designs of PBIED are command detonated by the suicide bomber. However, the bomb makers are now incorporating RC receivers and transmitters into future suicide vest designs to eliminate the suicide bomber's ability to surrender before detonation. These could then be activated by a trigger man from a safe distance.

24. **Person-Borne IED Backpack**. The Person-Borne IED Backpack (PBIEDB) consists of backpack containing an IED. The device usually does not use a radio controlled receiver or transmitter. Therefore, the individual wearing the backpack must be fully committed to the final outcome of the suicide operation. In order to stop the detonation of this device, prevention is to be applied by searches as well as frustrating the movement of materials.

METHODS OF RECOGNIZING IEDS/EXPLOSIVE ORDNANCES AND ACTIONS TO BE TAKEN

25. The reason for the prevalence of IEDs is the fact that they are cheap and relatively easy to make. They can be made from a whole range of materials, from everyday objects found in the home to commercial explosives used in construction and mining. They are also unique in nature because the IED builder improvises with available materials at any time. As IEDs become more sophisticated, they have become generally more difficult to detect and guard against. The effectiveness and sophistication of the IED depends largely on the experience, training and capacity of the terrorist as well as the materials used in the preparation of the bomb. An IED can be camouflaged to look like any ordinary object. This makes it very dangerous and difficult to detect. In the search for potential IEDs, everything that looks unusual or out of place should be suspected. Some of the tell-tale signs of impending IED attacks and suggested action to be taken shall be discussed.

26. **Recognition Signs for VBIEDs**. The identifying signs which may give away the game of a potential VBIED attack include but not limited to the following:

a. New tyres on old vehicles.
b. Airbag removed or deactivated.

c. Oil stains and tool markings on handle, steering wheel, dashboard, body or hood of the vehicle.

d. Headlamp or wiper on when it is not dark, foggy or raining.

e. Partially opened bonnet, especially at the end of the battery terminal.

f. Tinted windshield and windows, especially at the driver's and rear passengers' sides.

g. Hurriedly removed sound system with visible naked wires.

h. Power and relay switches at inappropriate places.

i. Tampered fuse compartment with extra cable connected.

j. Use of naked wound wires in place of rated fuse.

k. Overloaded vehicle, especially at the rear.

27. **Recognition and Apprehension of PBIED**.

Observable patterns which could aid in the recognition of PBIEDs include the following:

a. Attempts by persons to drop off packages and leave them unattended or throw bags into important facilities.

b. Suspicious bombers may be on foot or driving and attempting to gain access to barracks, facilities or restricted areas.

c. Inappropriate or bulky clothing to conceal explosives vest, bra, pants, cap or belt.

d. Robotic or difficult walk as they are carrying about 10-20 kgs of explosives with metals. Also some tend to be intoxicated before embarking on the mission, hence the funny walk.

e. Irritability, sweating or nervous behaviour may be

visible, depending on the degree of tunnelling or motive.

f. Low and controlled breathing, more or less like the bomber trying to regulate this so they do not get hypertensive.

g. Because of the tunnel vision and the need to block out any distraction, suicide bombers tend to stare straight ahead.

h. Mumbling or visibly moving lips without uttering of sounds.

i. An individual carrying an unusually large bag.

j. Hidden hands (in pocket, at the back or tucked inside the bag or clothes) or holding down an unknown object in the hand for a long period.

28. **Identification of Indicators of IED attacks**. The following are the precursor signs of impending IED attacks in a particular area:

a. Increase in car theft.

b. Theft of explosives and accessories.

c. Ammunition theft.

d. Fertilizer theft and diversion.

e. Cases of uncontrolled movement of explosives, accessories, fertilizer and precursor chemicals should be regarded as suspicious.

f. Cases of accidental explosions in residential areas.

g. Increased bank robbery.

h. Persons seen with items such as maps, cameras, binoculars, GPS, radio remote controllers may be suspected bombers.

i. Unknown persons taking photographs or making sketches of important facilities, barracks or restricted areas.

29. **Actions to be Taken on Observation of Suspicious IEDs**. On observation, members of the public are expected to report suspected IED cases to the nearest security outfit in order to guard against the resulting carnage. The ways of reporting suspicious IED attacks could include telephone calls through the national hotline which is '112' for Nigeria. Other means include making reports to media houses through letters or phone calls as well as making direct reports to the nearest security outfit. On receipt of such information, the security personnel are expected to take some recommended actions which are summarized by the 5 C's. The 5 Cs are Call, Confirm, Clear, Cordon and Control as follows:

a. **Call**. It is recommended that on receipt of suspected IED information, the Unit, higher authority or local authority (Government Officials, Fire service and other security agencies) be alerted immediately through any means available.

b. **Confirm**. Confirm whether item found is an IED, find out the precise location, the size and any obvious means of initiation. During the confirmation, the device is not to be handled and all are to maintain a safe distance from its location. If the IED is at a distance, confirmation could be used with the aid of weapon sight, binoculars and other surveillance assets. Also, use of communication near the site is to be avoided.

c. **Clear**. Once confirmed as an IED/possible IED, the area is to be cleared in order to protect life, ensure security and preserve evidence. All personnel as well as civilians are to be cleared immediately to a safe area.

d. **Cordon**. After clearing the area of any persons, the next thing is to cordon off the area. The purpose of a cordon is to control the area, maintain safety and allow clearance

operations. It is important to note the threat in such an incident could come from secondary devices, small arms/RPG fire or suicide bomber. A good cordon at the incident area should have depth, provide all round defence, satellite patrols and offensive posture as well as good communications amongst others.

e. **Control**. The incident commander must have firm control of the area before, during and after the arrival of other security force and agencies such as the police or military C-IED Team. The C-IED Team will select its own Command Post (CP) for operating and must have access to the device within the cordon. It is from the CP that the team will make its plans on how to defuse or safely blow up the IED so that normal activities can resume.

GROUND SIGN AWARENESS

30. Any evidence of change from the natural state that is inflicted upon the environment by the passage of man, animal or machinery are indicators of a possible IED threat in a theatre of operation. Environment plays a key part into the likely location of IEDs. Look out for signs of abnormal ground appearance. These ground signs are:

a. **Disturbance**. Area of compressed ground with loose disturbed surface.

b. **Discardables**. Items the enemy may intentionally or unintentionally leave behind at the emplacement site of an IED.

c. **Colour Change**. When the enemy emplaces an IED in the ground, the soil from the hole may differ in colour from the surrounding area due to the difference in moisture content below the surface.

d. **Transference**. Transference occurs when the IED

perpetrator takes soil, or any other material, from one area to conceal the IED at a separate location.

e. **Flattening**. Flattening is the general levelling or depression identified by the immediate surrounding area and colour change.

f. **Regularity**. Straight lines rarely exist in nature. When the enemy tries to conceal an IED some things appear out of place compared to nature's emplacement of soil, rocks, and vegetation. When the enemy buries or tries to conceal command wire, pull lines or trip lines, there is often a distinct line that would not naturally occur on the surface of the ground.

PRINCIPLES OF COMBATING THE IED THREAT

31. The following are the principles of combating the IED threats:

a. Keep an offensive mind-set. Always be ready for an IED encounter.

b. Maintain situational awareness.

c. Remain observant.

d. Avoid setting patterns.

e. Employ 360-degree security.

f. Maintain standoff from suspected IEDs.

g. Disperse soldiers and vehicles strategically.

h. Always use blast and fragmentation protection.

i. Take advantage of technology.

TEST QUESTIONS

1 What is an IED?

2 What are the basic components of an IED? Explain any

3 What are the various means of initiating an IED?

4 List the types of IEDs.

CHAPTER FOUR
NIGERIAN ARMY SIGNALS

INTRODUCTION

1. This guide is intended to assist officers preparing for the Captain to Major Written Promotion Examination. This reviewed module is produced with an input from HQ NAS. Passing the paper on military technology requires officers using this modules and also conduct depth reading of other materials to broaden their views on each topic. The purpose of this précis is to highlight the topics to be cover by candidates in preparation to Signal Exam.

TRAINING OBJECTIVES

2. After reading this précis, candidates will be able to explain the following:

a. Roles and Functions of NAS.
b. Equipment.
c. Communication Security.
d. Antenna Propagation.
e. Information Technology.
f. Electronic Warfare.
g. Maintenance Culture.
h. Signals Tactics.
i. Satellite Communication.
j. Cyber Security.
k. Documents Required for Comm Planning.
l. Radar System.
m. Unmanned Aerial Vehicle.
n. Closed Circuit Television.
o. NA ICT Policy 2016.
p. NAWANI.

REFERENCE AND MATERIALS

3. Candidates are also advised to consult and study relevant NAS books and pamphlets as well as NA ICT Policy 2016.

ROLES AND FUNCTIONS OF NAS

4. Candidates should be familiar with roles and functions of NAS. The NAS is responsible for the following:

a. Providing communication support to the NA.

b. Formulating and implementing policies on EW.

c. Formulating and implementing policies on ICT for the NA.

d. Management of NA radios and frequencies.

e. Maintenance and repairs of all communication and IT equipment in NAS inventory.

f. Training of officers and soldiers in communication and IT.

g. Research and development of communication systems.

h. Advise the COAS, Arm and Service on communication matters.

i. Liaison with civil institution/establishment on communication matters i.e Private Telecommunication Operators and NIPOST etc.

j. Additional roles and functions of NAS:

(1) Administration of NAWANI.

(2) Management of NA space communication.

EQUIPMENT

5. Candidates should be familiar with current equipment in use and should know the following:

a. **Qualities of Combat Net Radios.**

(1) Ruggedness.
(2) Security.
(3) Water proof.
(4) Ease of operation.
(5) Durability.
(6) Ease of maintenance.
(7) Compatibility /Interoperability.
(8) Reliability.
(9) EW Capability.

b. **Technical Details of Some CNRs in NAS Inventory**.

(1) **RF 5800 HH.**

(a) Type – VHF.
(b) Type of operation – Digital.
(c) Voltage – 12 VDC.
(d) Power output – 0.25w, 2w and 5w.
(e) Mode of operation - fixed, Hopping, Clone, Scan.
(f) Security – ECCM, COMSEC.
(g) Number of channels – 25.
(h) Number of spacing – 10KHz.
(I) Number of programmable Channel – 25.
(j) Weight – 3.4k
(k) Features – Clone Mode, Keypad, Lock Beacon Operation, GPS and COMSEC.
(l) Deployment – Section, PL, Coy and grd to air.
(m) Distance Coverage – Depends on the term and types of antenna used.

(2). **RF 5800V (MP).**

(a) Type – VHF.
(b) Type of operation – Digital.
(c) Freq range - 30 – 107.99MHz.
(d) Voltage – 23 – 30 VDC.
(e) Power output – 1w, 4w and 10w.
(f) Mode of operation – FM, FSK, TCM, CVSD.
(g) Modulation type – FM.
(h) Security – Encryption.
(i) Type of Antenna – Whip/blade.
(j) Number of Channels – 25.
(k) Channel spacing – 25KHz.
(l) Number of Programmable channel – 100 – 24 preset channels.
(m) Weight – 3.4kg.
(n) Features – Retransmit support FM voice, FSK, CVSD, TCM, KDU, Simplex and half duplex, GPS, BTT, Clone mode.
(o) Deployment – Coy – PL – Section level.
(p) Distance Coverage Depends on Antenna, terrain, weather and location.

(2) **RF 5800H Base Station.**

(a) Type – HF.
(b) Type of operation – Digital.
(c) Voltage – 26 VDC.
(d) Power output – 150w.
(e) Freq range – 1.6 – 59.99MHz.
(f) Mode of operation – fixed HOP, ALE, 3G and 3G+
(g) Modulation type – USB, LSB,

AME, CE and FM.

(h) Security – AVS, Citadel and datock encryption.

(I) Type of Antenna – Dipole.

(j) Number of channels – 200.

(j) Channel spacing – 100Hz.

(k) Number of Programmable Channel – 75.

(l) Weight – 18.7kg.

(m) Features – ALE, TOD, Encryption, LDV, Freq hopping, KDU, 3G+.

(o) Deployment – Bde – Div.

(p) Distance coverage – Depends on antenna, terrain, weather, location and freq.

(3) **RF 5800H (MP).**

(a) Type – HF

(b) Freq range 1.6 – 59.99MHz

(c) Voltage – 26 VDC (d) Power output – 1w, 5w and 20w(e) Mode of operation – fixed, HOP, ALE, 3G, 3G+, USB, LSB, AME, CE, FM.

(f) Security – freq hopping encryption, AVS, DATATEK.

(g) Type of Antenna – Whip (20Ft).

(h) Number of channels – 200.

(I) Number of programmable channel – 200.

(j) Weight – 4.5kg.

(k) Feature – GPS, wireless internet protocol data transfer, LDV.

(l) Deployment – Bn, Coy and Pl.

(m) Distance Coverage – Depends on

Antenna, terrain, weather, location and freq (14km).

(4) **RF 5000.**

(a) Type – HF.
(b) Type of OP – Digital.
(c) Freq range – 1.6 – 29.99MHz.
(d) Voltage – 24 VDC.
(e) Power output - 125w.
(f) Mode of OP – fixed.
(g) Modulation type – USB, LSB, AME, CW.
(h) Security – ECCM, Comsec.
(i) Type of Antenna – Dipole.
(j) Number of channel 100.
(k) Number of programmable channel – 75.
(l) Weight – 34kg.
(m) Features – ALE.
(n) Deployment – Div – AHQ level.
(o) Dist Coverage – Depends on antenna, terrain, weather, location and freq used.

(5) **Codan HF.**

(a) Type – HF.
(b) Type of OP – Digital.
(c) Freq range – 1.6 – 30MHz.
(d) Power output – 25w.
(e) Voltage – 12 VDC.
(f) Modulation type – USB, LSB, AM.
(g) Security – hopping, voice encryption.
(h) Type of Antenna – Whip, long wire, slopping and Dipole.
(I) Number of Channel – 200.

(j) Number of programmable channel – 200.
(k) Feature – GPS, ALE, LOA, Data Comm.
(l) Deployment – Bn – Bde.
(m) Dist Coverage – Depends on terrain, location, weather and freq.

(6) **Matador HF Base Station.**
(a) Type – HF.
(b) Type of operation – digital.
(c) Freq range – 2 -30MHz.
(d) Voltage – 24 VDC.
(e) Power supply – 500w.
(f) Mode of op – Hop and fixed.
(g) Security – Hopping and COMSEC.
(h) Type of Antenna – Broadband.
(i) Number of channel – 2 – 256.
(j) Channel spacing – 25KHz.
(k) Number of programmable channel – All.
(l) Weight – 43kg.
(m) Features – selcal, telcal, beacon, scan bit and squelch.
(n) Deployment – Div and above.
(o) Distance Coverage – on limited.

(7) **Other Radios in NAS Inventory.**
(a) PRC 2080 VHF.
(b) PRC 9800 HF.
(c) RF 2301.
(d) RF 350K.
(e) TRA 931.
(f) AVRC 83.

(g) GP 380 HHR.
(h) CP 200 HHR.
(i) CP 180HHR.
(j) HT 750.
(k) GP 340 HHR.
(l) Matador MP HF.
(m) Matador VHF (Base).
(n) AN PRC 117A Transceiver.
(o) Redifon.
(p) Datron (PRC 1099A MP).
(q) VRC 301 MP.
(r) VRC 94A.
(s) VRC 301 Vehicular.
(t) RT 351/352 Transceiver.

i. **Characteristics of HF Radio**.

(1) Extensive range depending on the aerial.
(2) Useful for long range communication.
(3) Less susceptible to screening due to skywave propagation.
(4) Highly vulnerable to electronic counter measures (ECM).
(5) Tremendous frequency congestion.
(6) Require high power
(7) Can be affected by skip distance.
(8) It is propagated through sky wav
(9) Freq range of 3 – 30MHz.

j. **Characteristics of VHF radio**.

(1) Useful for short range communication.
(2) Susceptible to screening.

(3) Less affected by atmospheric noise and interference.
(4) Used LOS technology.
(5) Low power req.
(6) Freq range 30 – 300MHz.

k. **Characteristics of UHF radio**.

(1) Smaller and less conspicuous antenna.
(2) Susceptible to screening.
(3) Useful for short range communication.
(4) Less affected by atmospheric noise and interference.

l. **Lines Communication Equipment**.

(1) **Types of Cable**.

(a) D 10.
(b) L 244.
(c) Coaxial cable.
(d) Armoured cable.
(e) D 8.
(f) D 3.
(g) PVC 100.
(h) PVC single pair.
(i) PVC 10 pair.

(2) **Types of Exchange/Lines Comm Eqpt**.

(a) 10 Lines magnetor.
(b) 15 Lines magnetor.

(c) 50 Lines magnetor.
(d) SB 3082.
(e) Redcom exchange.
(f) PABX Panasonic.
(g) F/F (field and faultress) Switch Board.

(3) **Types of Exchange Handset.**

(a) Field telephone.
(b) Linesman telephone.
(c) Digital telephone.

m. **Advantages of Lines Comm.**

(1) Not susceptible to screening.
(2) No interference.
(3) It does not req RF to operate.
(4) Best means of communication in def.
(5) Cheaper than radio comm.
(6) Less danger (no ATU).

n **Disadvantage of Lines of Comm**.

(1) Can be damaged by an animals or track of tank.
(2) Can be damaged by explosion or fall of shot.
(3) Track of tanks or heavy duty vehicle could damage it.
(4) Fatigue in laying the lines.
(5) Can be easily tapped.
(6) Subscriber cannot be reached if engaged.
(7) Lines are not use in mobile system of communication.
(8) Voice conversation cannot be concealed due to

use of plain language between subscribers.

o. **Land Mobile Radio (LMR).**

(1) **LMR Freq Ranges.**

(a) **V H F .**
(i) **Range 1.** 154MHz. 132 –
(ii) **Range 2.** 174MHz.
(b) **UHF.** 120 –
(i) **Range 1.** 433 MHz. 403 –
(ii) **Range 2.** 470 MHz. 433 –
(iii) **Range 3.** 494 MHz. 470 –
(iv) **Range 4** 520 MHz. 494 –

p. **Components of Repeater System.**

(1) Repeater Housing.
(2) Fan Assembly.
(3) Power Supply.
(4) Repeater Controller.
(5) Receiver Radio.
(6) Transmit Radio.
(7) Repeater Interface.

p **Programming Kits for LMR.**

(1) A clean and uncorrupted computer system reserved for only the purpose.
(2) Software version of particular repeater to be programmed.
(3) USB – Serial Adapter.
(4) RIB – to connect the radio link to the board and to the computer.
(5) Power supply source for the RIB.

(6) Cable connections between RIB and Computer to the radio link.
(7) A robust type of connector with universal plugs for various types of radio.
(8) A steady power supply.

r. **Components and Accessories of LMR.**

(1) Suitable Repeater System.
(2) Duplexer.
(3) Antenna feeder cable of various grade.
(4) A high mast of 150 – 250 ft height.
(5) Guide Rope.
(6) Inverter system or solar system as alternative source of power supply.
(7) Heavy duty battery (deep cycle).
(8) Connectors for cable.
(9) Thunder Arrestor.
(10) Appropriate HHR.
(11) Appropriate veh base radio.
(12) Radio link.
(13) Solar Changer Control.
(14) Base /Diamond antenna.
(15) Robust Programming Kit.
(16) Pilot Light Indication.

COMMUNICATION SECURITY

5. Candidates should cover the followings:
a. **Spectrum Monitoring.** Spectrum monitoring is a process used to detect interfering and unauthorized RF transmissions, monitor emergency frequencies, protection of large area as well as high-value assets such as airports, seaports, industrial and educational campuses. Spectrum monitoring solutions let you measure, analyze and locate

traditional and modern signals and address the challenges of crowded and complex signal environments. Spectrum monitoring models range from LF, HF, VHF, UHF, SHF and EHF. The architect design of spectrum monitor facilitates frequency, bandwidth, modulation depth, field strength, direction finding and geo-location measurements. Spectrum monitoring therefore serves as the eyes and ears of the spectrum management process.

b. **Purpose of Spectrum Monitoring.** The measured spectrum occupancy is useful information for the following:

(1) Planning, engineering, and enforcing new spectrum sharing and relocation scenarios.

(2) Measured spectrum data could be made available alongside license and assignment data to improve the quality and quantity of information available for planning by policy makers, spectrum managers, and investors.

(3) In the engineering phase of a transition process, real-time and historical measured spectrum data could be used to check assumptions, validate propagation and usage models, and field test dynamic coordination schemes and technologies.

(4) Open and transparent use of relevant spectrum data can play a critical role in interference resolution and enforcement in the increasingly dynamic and complex interference environment.

(5) Another purpose of spectrum monitoring is to support the spectrum management process in general, including frequency assignment and spectrum planning functions.

c. Subdivision of Communication Security. The Comsec involve the following measures, subdivisions or components:

(1) **Transmission Security.** Transmission security is the component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by frequency hopping and spread spectrum or through crypt analysis. It is also a protective measure design to deny the adversary information from interception, DF, Monitoring and analysis. Transmission security include: (a) Spread spectrum techniques. (b) Electromagnetic control. (c) Protective procedure. (d) Efficient spectrum management.

(2) **Physical Security.** Physical security is the component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access by unauthorized persons. The physical security involve the protection of physical elements of communication system, cipher eqpt and document. The following ways could be used to achieve efficient physical security measures:

(a) Proper manning of vehicles.
(b) Proper manning of radio stations.
(c) Securing CEI.
(d) Destroying of CEI, equipment and key materials in an event of capture.
(e) Concealment of CP.
(f) Camouflage and concealment of mast, vehicle, equipment and antenna.
(g) Security of codes, ciphers and cryptographic equipment.

(h) Use of password and authentication.
(i) Security lock/use of pad lock.
(j) Alarm system.
(k) Electronic fence.
(l) Educate personnel.

(3) **Cryptographic Security**. This is a measure design to prevent, reduce or deny the use of own cryptographic information code or ciphers. The cryptographic security is the component of communications security and also involve the provision of technically sound crypto systems and their proper use. This includes ensuring message confidentiality and authenticity.

(4) **Operations Security.** Operations security is a process that identifies critical information to determine if friendly actions can be observed by adversaries' intelligence and determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

(5) **Information Security.** This is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take**.**

(6) **Radiation/Emission Security**. This is the

protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from communications systems and cryptographic equipment intercepts and the interception and analysis of compromising emanations from cryptographic equipment, information systems, and telecommunications systems. This are measures design to prevent the enemy from obtaining information through interception of electromagnetic energy, radiation or emission. Under this, operators should know the following:

(a) Minimum power.
(b) Appropriate antenna.
(c) Authorize code.
(d) Authorize procedure.

(7) **Personal Security**. The personal security deal with vetting of operator as well as cryptographic clearance for codes and ciphers users including users' responsibilities.

ANTENNA PROPAGATION

6. Candidates should cover the following:

a. **Types of antenna**.

(1) Whip antenna.
(2) Dipole antenna.
(3) Yagi antenna.
(4) Omni directional.
(4) Directional.
(5) Parabolic antenna.
(6) Invented V antenna.

(7) Vertical rod antenna.
(8) Blade antenna.
(9) Slopping Antenna.
(10) T – Shape antenna.
(11) Vertical wire antenna.
(12) Ground wire antenna.
(13) VHF/UHF bi – conical antenna.
(14) Telescopic antenna.
(15) Broad band antenna.

b. **Fading**. Fading is a process whereby a received signal varies in intensity over a short period of time. It is one of the problem experiences in sky wave communication.

c. **Causes of Fading.**

(1) Interaction of 2 parts of the same radio wave which have travel in different paths.
(2) Violet changes in the ionosphere.
(3) When the sky wave and ground wave produced arrive at the receiver at the same time.

d. **Types of Fading.**

(1) **Interference Fading**. The interference fading is caused by phase interference of two or more waves from the same transmitter arriving at the same receiver.

(2) **Polarization Fading**. This is as a result of change in state of polarization of down coming wave relative to the orientation of receiving antenna which causes variation in the field intensity.

(3) **Absorption Fading**. It is caused by the short time variation in the amount of absorption in the atmosphere.

(4) **Skip Distance Fading**. This occurs at places near the limit of the skip distance and is caused by the changing angle of reflection.

e. **How to Reduce Fading.**

(1) The use of Automatic gain control in the receiver.

(2) Increasing transmitter power.

(3) The use of diversity reception system.

f. **Effects of Jungle /Vegetation and Terrain on VHF Signal**.

(1) **Effects of Jungle /Vegetation.**

(a) Impenetrable mangrove swamps and jungle affect propagation of signal particularly ground and direct waves.

(b) Hot Jungle weather can affect the performance of equipment. This can affect the strength of the signal produced. High temperature therefore lower equipment performance.

(c) Humid in vegetation area tend to be hot. This can affect the propagation and strength of the signal.

(d) In highly jungle or vegetation terrain, storm usually prevail during raining season. This can affect communication equipment if not well earthen. This can in turn reduce eqpt

performance resulting in fluctuation of signal.

(e) Highly Vegetation/Jungle terrain result in troop's fatigue. This can lower the troop's efficiency to operate the equipment. This can in turn affect the propagation signal.

(f) Jungle climate is capable of making the life of dry battery for HHR much shorter.

(g) Poor Atmospheric condition in jungle/ vegetation terrain amount to weak signal.

(h) Dense jungle/vegetation led to screening effect.

(2) **Effect of Terrain.** The Mountainous, maritime, desert, urban as well as jungle terrain affect signals communication in one way or the other as follows:

(a) **Maritime Terrain**. The maritime terrain affects signal communication as follows:

(i) The water line affects radio frequency propagation.

(ii) Doppler effects.

(iii) Diurnal variation affects radio frequency propagation.

(iv) The weather change in maritime environment (ice, waves, water temperature) affects signal propagation.

(v) Wet, dew and moisture reduce equipment performance which affect signal propagation.

(b) **Mountainous Terrain.** The mountainous terrain affects signal communication as follows:

(I) Hills and valley affect LOS communication and drastically reduce the strength of the signal.

(ii) Mountain can give rise to forest which affects the signal propagation.

(iii) The hills can sometime give rise to snow depending on the area or region. This also have effect on the signal propagation.

(iv) Mountainous and hilly terrain affects the movement of communication vehicles. This can affect the distance cover accordingly.

(v) The humid heat of the day is often received by the cool air in the late evening from the mountain giving rise to fluctuation of signal strength.

(vi) High dew temperature degraded personnel efficiency which reduces their ability to operate the equipment effectively, this affect signal propagation.

(vii) The effect of lightening or thunder could damage the equipment and this can affect the ability of the personnel to achieve efficient propagation of security.

(c) **Desert Terrain.**

(i) Highly day temperature degraded the effect of human efficiency to operate the equipment. Hence this may affect the signal

propagation.

(ii) Effects of bad going for communication vehicle is capable of reducing the strength of the signal.

(iii) High temperature rate can reduce radio frequency signal which affected the propagated signal.

(iv) Effect of wind and sand make orientation and direction keeping increasingly difficult. This could affect signal propagation for LOS communication.

(v) Wind and blown sand can affect performance of equipment, hence reducing or affecting signal generated for communication. (vi) Thunderstorm and lightning strike is a serious hazard in an open desert area which affect signal propagation

(d) **Jungle Terrain.**

(i) Dense tropical grow and trees affect propagated signal particularly direct and ground wave.

(ii) Impenetrable mangrove swamp affect both men and equipment their by affecting radio frequency of radio signal.

(iii) Jungle weather tends to be hot which affect the performance of propagated signal. (iv) High humid condition in the jungle reduces signal

strength.

(v) Troop fatigue in jungle operation tend to lower their efficiency. This if not manage properly could affect equipment handling which could affect signal propagation.

(vi) Poor atmosphere condition amount to weak and fluctuation of signal in jungle terrain.

(vii) Dense terrain in a given jungle could led to screening effect.

(viii) Movement of communication vehicles tend to be difficult. This is a problem in LOS Communication when trying to align the transmitting and receiving ends.

(viiii) Screening effect of foliage affect radio signal performance.

(x) Radio Communication is very difficult at night due to the fluctuation of signal and weak signal strength.

(e) <u>Urban/BUA Terrain</u>.

(i) The Urban terrain composed of angular form in plain nature patterns. This could affect LOS signal.

(ii) Stretching of communication resources in BUA tend to reduce the strength of the propagated signal.

(iii) Large city provide serial of planes of urban high ground which can affect LOS signal for LMR.

(iv) In an ops, communication vehicles

are front to ambush and attack in all direction. The zeal by operators to deploy the FFR to achieved proper LOS for smooth propagated could be obstruct or hamper.

INFORMATION TECHNOLOGY

7. Candidates are to be familiar with the following:

a. **What is a Computer**. A computer is a set of electronic equipment that accepts data as input, process them with the aid of predefined instruction called program and produces useful output for management use.

b. **Characteristics of Computers.**

(1) Cost
(2) Speed.
(3) Storage and capacity.
(4) Security and protection.
(5) Quality job.
(6) More info.
(7) Relevant.
(8) Supply result to user.
(9) Accuracy.
(10) Reliability.
(11) Power consumption.

c. **Components of Computer**. The component units of computer system includes:

(1) Input Device.
(2) Output Device.
(3) Processing Unit.
(4) ALU.

(5) Primary Memory.
(6) Secondary Memory.

d. **Computer software.** Computer software is a program and instructions that can use the hardware to work or carry out its tasks. They are used to manipulate and govern how the hardware is utilized. The software control the interaction between input and output devices, software cannot be touched or feeled with hands. The software is also refered to as internal component of the computer. It main action is to enhance and control the activities of the computer. The factors that determine the choice of software are:
(1) Speed.
(2) Size.
(3) Cost.
(4) Reliability.
(5) Storage.

e. **The Categories Software.**
(1) System software.
(2) Application software.

f. **Computer Hardware**. Computer Hardware are device or equipment involved in the functioning of computer. They are components that can be physically handled. The functioning of this components is typically divided into 3 main categories as follows:
(1) Input Device.
(2) Output Device.
(3) Processor.

g. **Examples of Input Device.**

(1) Keyboard.
(2) Card reader.
(3) Mouse.
(4) Joy stick.
(5) Scanner.
(5) Light pen.
(7) Voice input/Mic.
(8) Monitor/touch sensing display.
(9) Punch paper tape reader.
(10) Optical character recognition.

h. **Examples of Output Device.**

(1) Monitor.
(2) Printer.
(3) Speaker.
(5) Projector.
(6) Headphone.

I. **Examples of Storage device.**

(1) Permanent Storage eg RAM and CD ROM.
(2) Temporary Storage eg RAM.

j. **Information Storage.** The information Storage is the systematic way of storing data so that they can be located and displayed when required or requested. The information can also be classified as having been stored to or retrieved from primary or secondary memory. The primary memory is the computer main memory while the secondary memory is any form of memory other than the main memory e.g hard disks, floppy disks, CD Rom and magnetic tape.

k. **Storage Media.** The storage media is a device for storing information, Information is stored in many types of media the most common being used are:

(1) Floppy disk.
(2) Hard drive.
(3) CD Rom.
(4) Magnetic tape.

l. **List of Some Applications Packages and Programs.**

(1) Microsoft Word.
(2) Microsoft Excel.
(3) Microsoft Access.
(4) Microsoft Publisher.
(5) Word Perfect.
(6) Corel Draw.
(7) Qbasic.
(8) C++
(9) Page Maker.
(10) Visual Basic etc.

m. **Applications of Computer.** Some of the military and misc applications of computer is given below:

(1) **Military Applications.**

(a) Training and education.
(b) Communication system training.
(c) Simulation and war gamming.
(d) Creating data base for data management system.
(e) For keeping sensitive document.
(f) Use in the area of logistic to support propose supply and procurement.

(h) Given the degree of efficiency and effectiveness of military lops.
(i) Network centre Warfare and battle field situation awareness.
(j) Decision making process.
(k) Lunching of satellite.
(l) RISTA
(m) RADAR technology.
(n) R & D.
(o) Use in combat aircraft for target acquisition.
(p) Use for meteorology.
(q) Use for encryption technique.
(r) Use in weapon system.

(2) **Misc Applications.**
- (a) **Education.**
  - (i) Computer aided leaning.
  - (ii) Dist leaning.
  - (iii) Online exam.
  - (iv) Online training.
- (b) **In Business.**
  - (i) Marketing.
  - (ii) Stock exchange.
  - (iii) Shopping.
- (c) **Medical Services.**
  - (i) Diagnosis.
  - (ii) Life support system.
  - (iii) Patients monitoring.
  - (iv) Hospital management system.
- (d) **At Home.**
  - (i) Home budget.
  - (ii) Games.
  - (iii) Entertainment.

(iv) Chatting.
(vi) Information.
(v) Shopping.

o. **Computer Network**

(1) **Internet.** Internet is a worldwide network base on the series of interconnected network for the purpose of sharing of information and resources.

(2) **Intranet.** Intranet are the same technology as the internet. It is typically the implementation of LAN and WAN connected together.

p. **Network Components.**

(1) Transmission medium.
(2) Clients.
(3) Server.

q. **Network Design**. Every network design leverages on the 4 fundamental network design goal as follows:

(1) Scalability.
(2) Availability.
(3) Security.
(4) Manageability.

r. **Computer Networking.** This is the interconnection of computers for the purpose of sharing of information and resources.

s. **Types of Computer Networking.**

(1) **LAN**. The LAN are computer connected together within a local area eg an office or home.

(2) **WAN**. In WAN, the computer are further apart and are connected to use telcomms eqpt and communication line or radio eqpt. It exceed a distance

of 2km from end to end. It is the connection of series of LAN.

(3) **MAN**. The MAN involve the interconnection of series of LAN and WAN.

ELECTRONIC WARFARE

8. Candidates should know the following:

a. **Electronic Warfare.** Electronic Warfare is an action or process that involve the effective use of electromagnetic energy, emission or radiation on the adversary thereby preventing, denying or reducing the effective use of same electromagnetic spectrum by the adversary.

b. **Objectives of Electronic Warfare**.

(1) Protection.
(2) Disruption.
(3) Detection of emission.
(4) Locating of emission.
(5) Identification of emission.
(6) Analysis of data.
(7) Data extraction.
(8) Jamming.
(9) Deception.
(10) Support wpn system.

c. **Elements of Command and Control.** The EW takes its rightful place within the elements of C2 Due to its ability to dominate the battle space. The elements of C2 are as follows:

(1) Operational security.
(2) EW.
(3) Psychological operations.
(4) Deception.
(5) Physical destruction.

d. **Components or subdivisions of Electronic Warfare.** The subdivision of EW are:

(1) Electronic Support or Electronic Support Measure.

(2) Electronic Attack or Electronic Counter Measure.

(3) Electronic Protection or Electronic Counter Counter Measure.

(a) **Electronic Support**. This is the division of EW that involve action taken to search for, intercept, identify and locate the source of intentional and non-intentional radiated electromagnetic emission for the purpose of immediate threat recognition, planning, targeting and conduct of furtive battle. The Electronic support information is used for:

(i) Direct Action Ops.

(ii) Support Electronic Protection efforts.

(iii) Create EW data base.

(iv) Modify EW data base.

(v) Exploit enemy emission.

(vi) Support information ops.

(vii) Provide information on enemy capability and intent.

(viii) Tasks Wpn system.

(b) **Electronic Attack.** Electronic Attack is a division of EW that involve action taken to prevent, deny, or reduce the effectiveness of enemy electromagnetic energy or emission thereby using same energy to attack enemy equipment, facilities and

resources through jamming, deception, neutralizations as well as destruction with the intent of degrading, neutralizing or destroying adversary combats capability.

(c) **Electronic Protection**. This is the division of EW involving passive and active measures taken to protect personnel, Eqpt and facilities from effect of adversaries' electromagnetic spectrum and to ensure friendly employment of EW or electromagnetic spectrum that may degraded, neutralize or destroy adversaries' combat capability. it is designed to protect friendly combats capability against undesirable effect of friendly or enemy employment of EW.

e. **Ways of Accomplishing Electronic Protection.**

(1) Selection of scheme of maneuver that will minimize and disrupt Electronic Support or Electronic Attack.

(2) Simple scheme of maneuver that can be executed with few emissions.

(3) By imposing radio silence.

(4) By adopting measure to minimize jamming.

(5) By reducing transmission power.

(6) Through brevity of transmission.

(7) Using directional antenna.

f. **Roles of EW Staff.**

(1) Coord of the activities of EW Cell.

(2) Developing EW concept.

(3) Synchronizing of Electronic Support, Electronic

Attack and Electronic Protection.

(4) Developing supportive plan.

(5) Plan and coord EW activities.

(6) Create and modify EW data base.

g. **SIGINT, COMMINT and ELINT**

(1) **Signal intelligence**. Signal intelligence is the category of int comprising either individual, combination of commint, electronic int or foreign Int. SIGINT is also the int gather through interception of comm. between 2 parties using cryptanalysis. The SIGINT is further subdivided into 2 namely COMMINT and ELINT.

(2) **Communication Intelligence.** COMMINT is defined as intelligence obtain through interception by an intended recipient. It is therefore the int obtain by interception of signal between people or between2 parties. It is derive from the study of enemy sig comm and is used in the production of battle int and strategy int. The info obtain from COMMINT include:

(a) Adversary Identity.

(b) Adversary Loc.

(c) Adversary ORBAT.

(d) Adversary State of readiness.

(e) Adversary Activities.

(f) Adversary Future Intentions.

(g) Adversary Composition.

(h) Adversary Strength.

(I) Adversary Morale

(j) Adversary Combat Capability.

(k) Adversary Combt Efficiency.

(l) Adversary Scheme of Maneuver

(m). Adversary Wpn.

(3) **Uses of COMMINT**.

(a) Targeting for neutralizing, destruction and exploitation.

(b) Create and modify EW data base to steer Electronic Attack.

(4) **How to Prevent Adversary From Obtaining own COMMINT.**

(a) Concealing the structure of the comm network.

(b) Concealing content of traffic using codes and ciphers.

(5) **Electronic Intelligence**. This is the system of collecting RADAR emission data or electronic signal not directly used in comm. Hence, ELINT is the system of collecting virtual parameters of non comm system such as emission, radiation and energy from eqpt such as RADAR, antenna and Mast. The information obtain from ELINT may include amongst other the following:

(a) Types of RADAR use by the adversary.

(b) Location of the RADAR.

(c) Adversary electronic orbat.

(d) Important parameters of non comm system.

f. **What is Jamming.** Jamming is a process involving the use of a device or jamming signal to intentionally create interfering radio signals to effectively jam transmitting device so as to be unable to transmit effectively.

g. **Types of jamming.**

(1) Spot Jamming.

(2) Barage Jamming.

(3) Swap Jamming.

(4) Comb Jamming.
(5) Acoustic Jamming

h. **Commonly Used Jamming Signal.**
(1) Random noise.
(2) Stepped tones.
(3) Spark.
(4) Gulls.
(5) Random pulse
(6) Wobbler.
(7) Recorded sounds.
(8) Preamble jamming.
(9) Sweep jamming.
(10) Random keyed CW.
(11) Keyed CW
(12) Rotary.
(13) Random keyed modulated CW.

j. **Jammer Transmitting Station.**
The complete jammer transmitting station should include the following:
(1) The jammer transmitter with loud speaker.
(2) A type recorder.
(3) A receiver for monitoring.
(4) A radio receiver for recording the jamming signal.
(5) A means of communication with control of the jammer net.

k. **Techniques in Preventing Jamming.** The techniques of overcoming jamming includes:
(1) Freq diversity.

(2) Space diversity.
(3) Space spectrum.
(4) Freq hopping.
(5) Trg of ROPs and signal staff in what to do in jamming situation.
(6) The use of software to remove the frequency (excision).

l. **Types of Anti jamming Drills**. The 2 types of anti-jamming drills are:
(1) Unit anti jamming drills.
(2) Operational anti jamming drills.

(a) **The Unit Anti Jamming Drills is as Follows**.
(i) The first thing is to remove the radio coax to determine whether or not the interference is cause by an incoming signal.
(ii) If jamming occurred the operator initiates the unit anti jamming plan as contained in the unit Electronic Protection plan.
(iii) The next is to listen to the signal to try to discover the cause of the jamming as follows:
(aa) Music will imply jamming.
(bb) Voice may indicate that someone is on the net. Once you determine that it is a jamming signal, you then carry out the following:

(aaa) Carry out operator jamming drills.

(bbb) EW JAMREP send. If the net cannot work on VHF and the operator cannot control the net, the operator carry out the following:

(aaaa) Move to the next nominated spare freq.

(bbbb) If the first nominated spare freq suffer the same set back, move to the tune freq changing plan on the CEI.

(cccc) Based on the advice by the RSO/OC/CO the control operator can move to the net freq as reflected in the CEI for that time of the day.

j. **The Operator Anti Jamming Drill.**

(1) Remove the coax to determine whether or not jamming occur.

(2) Resite your antenna station.
(3) Try relaying.
(4) Increase power (temporary).
(5) Change freq.
(6) Prepare to send EW JAMREP.

k. **How to Reduce Jamming**.

(1) Strictly adhere to Comsec.

(2) Simulation of radio traffic to deceive the enemy.

(3) Cease transmission long enough so as to deceive the enemy as if there is sudden change in freq.

(4) Use of Morse.

(5) Reduction in number of transmission using data comm.

(6) Avoid sending long message.

(7) The use of robust contingency plan for those responsible for setting of radio comm. in case of jamming.

l. **Human Consciousness in a New Environment**.

To achieve a reasonable measure of combat success in an EW environment, there must be some consciousness; the candidates should know the following:

(1) The electromagnetic spectrum is free to both friendly and hostile forces, depending on EW asset employed.

(2) EW could be an effective weapon of warfare if effectively employed.

(3) All electromagnetic emission are potentially sources of information to the enemy.

(4) Communication in plain voice over combat

radio must be avoided as much as possible. Codes, call-signs, nicknames etc to be used as appropriate.

(5) Net discipline and correct procedures is essential in a combat net.

(6) Keep emission to the barest minimum – use data in HF communication.

(7) Need to vet personnel involved in communication.

(8) Combat communication assets should be physically secured against unauthorized persons. (9) Waste paper captaining any service information must be burnt under supervision.

(10) A potential enemy has the capability of always listening into all electronic transmissions.

(11) Passive and active EW measures must not be ignored.

(12) Combat communication must be allowed to fall into enemy hand intact during operation.

(13) Need for liaison with all services to ensure on integrated EW system.

MAINTENANCE

8. After detailed study, candidates should be familiar with the following:

a. **Maintenance Procedure**. The maintenance procedure in NAS involve the following:

(1) The Bde Sig have the technical maintenance troop outfit that assist in handling the repairs and maintenance of equipment within the Bde as well as maneuver units and supporting elements. If the bde sig cannot handle the repair, the eqpt is backloaded to the Support Regiment under Sig Bde for further action.

(2) The Support Regiment handle the repair within the Sig Bde (Div Sig) and those eqpt that cannot be handle by the Bde Sig. When Support Regiment repair the backloaded eqpt from the Bde Sig, the eqpt is send back to the Bde Sig while if the repair is beyond the Sig Regt, the eqpt is send to 57 Signal Maintenance Command for further action.

(3) The eqpt are forwarded to 57 Maintenance Command with complete accessories for further diagnosis and possible repair. When the eqpt are repaired, they are sent back to the supporting regiment accordingly.

b. **Maintenance Documentation**. The following document are found in technical workshop in support of repair and maintenance as well as record keeping:

(1) AF 1045 – Svc sheet.
(2) Eqpt job card.
(3) Daily Maint card.
(4) Monthly Maint card.
(5) Modules analysis sheet.
(6) Eqpt history card.
(7) Modification Card.
(8) Calibration record sheet.
(9) Spare requisition sheet.
(10) Workshop performance chart.

c. **Types of Maintenance**. The 4 types of maintenance are:

(1) **Prevention maintenance**. The preventive maint is the care and servicing of the eqpt and facilities bypersonnel for the purpose of

maintaining them in satisfactory operating condition. It can be achieve through:

(a) Inspection of the device or eqpt.

(b) Detection of fault.

(c) Correction of fault before they occur.

(2) **Catastrophic Maintenance**. The catastrophic maintenance is a maintenance carry out to effect major repair or overhauling of eqpt or facilities in order to achieve reliability and for the purpose of bringing the eqpt or facilities back to satisfactory condition.

(3) **Daily Maintenance**. The daily maintenance is one carried out either weekly, monthly, 3 monthly , 6 monthly, 9 monthly or yearly for the purpose of keeping the eqpt in good shape and satisfactory condition.

(4) **Corrective Maint**. Corrective maintenance in both war and peace time is carried out to repair the defects revealed during preventive maintenance. In order to ensure efficient repair of broken down comm equipment in peace time, NAS has four lines of maintenance supports as follows:

(a) **First Line Sp.** The first line support is carried out in the TM workshop of the Bde Sig. It include daily cleaning, lubrication of parts, minor electronic fault finding, changing of fuses, repair or replacement of handsets and replacement of faulty connecting cables and accessories among others.

(b) **Second Line Support**. Second line

support repairs are carried out by the TM workshop of Sp Regt, at Sig Bde level [Div sig level]. It covers all aspects of first line repair including specialised re-caliberation of equipment, component level repairs and replacement of modules and carrying out major electronic fault finding.

(c) **Third Line Support**. Third line support repairs are carried out in 57 SC on equipment that cannot be repaired at the second line sp. This level of maintenance is carried out by highly specialized technicians and it involves complex re-calibrations, replacements of major components and modules, refurbishment, gen overhauling of equipment, redesigning and rebuilding of equipment and complex electronic fault finding.

(d) **Fourth Line Sp**. Fourth line repairs are carried out to restore the equipment to new condition, to build new equipment out to fabricate equipment parts. This level of repairs include radio fitting and is done by 57 SC in collaboration with NAEME, equipment vendors and research institute within the AFN such as NASDC.

(5) **Corrective Maintenance In War Time.** In war time, the overall goal is to ensure that broken

down equipment including the CNR's are repaired in-situ or as far forward as possible in the combat zone. Consequently, 3 levels of maintenance sp in war time were considered in the proposed NAS equipment maintenance policy. This include the following:

(a) **Sig Fwd Repair Gp.** The sig fwd repair gp is organized to carry out priority of second line repair in fwd unit. The Sig Fwd Repair Gp would support a Mech Bde SP area. The sig fwd repair gp would be split into 3 sig fwd repair teams each supporting a battalion in the Bde.

(b) **Sig Fwd Repair Team**. The sig fwd repair teams is organised to carry out first line repair or replacement of communications equipment in the theatre of operations. The repair team will be detached from repair gp to directly support a mnvr unit.

(c) **Sig Maint Repair Gp**. The sig maint repair gp consist of the entire bde sig less the sig fwd repair group and will be equipped with mobile workers so as to facilitate the mobility of the sig fwd repair gp and various sig fwd repair teams. Faulty equipment that could not be repaired in the field will be back loaded to sig bde [Div level] support regt and 57 SC accordingly.

d. **Challenges of Equipment Maintenance in NAS.**

(1) Nonexistence of NA equipment maintenance policy.

(2) Lacks of standardization of NAS equipment.

(3) Poorly articulated NA equipment procurement

policy.

(4) Death of skilled technicians.

(5) Lack of diagonosis and repair tools.

(6) The complexity of the new set of digitalized radio in NA Inventory such as RF 5800, PRC 5800 make component level repair difficult.

e. **Strategies for Enhancing Equipment Repair in NAS.**

(1) Review of proposed NAS equipment maintenance policy.

(2) Enhanced incentives for technicians.

(3) Increased funding of NA equipment maintenance.

(4) Adoption of defense offset procurement system to cater for technology transfer.

(5) Establishment of radio assembly and manufacture centre in NAS.

SIGNAL TACTICS

9. The candidates should be familiar with following areas:

a. **Principles of Signal Communication.**

(1) Chain of command.

(2) Integration and interoperability.

(3) Anticipation.

(4) Reliability.

(5) Flexibility.

(6) Economy.

(7) Security.

(8) Speed.

(9) Survivability.

(10) Technical admin.

b. **Why Hqs Move.** HQs will generally move for one of the following reasons:

(1) As a result of direct adversary action.

(2) As a protection to counter adversary reconnaissance or direction finding.

(3) Because of bad sitting or poor communication.

(4) To close up with forward troops who could be advancing fast or have gained ground in order to control the battle better.

c. **The Grouping for Movement of Hqs.**

(1) Reece group.

(2) Rover group.

(3) Main hq which is regroup into:

(a) Main G Ops.

(b) Main Support.

(4) G 6 Cell which is regroup into:

(a) G6 Main (Sig Main).

(b) G6 Support (Sig support).

(5) Admin Area Group which is regroup into:

(a) Layout group.

(b) Main body.

d. **Recce Gp.** The recce group is subdivided into reece and layout elements. The composition of the Reece and layout elements is as follows:

(1) **Reece Elements.**

(a) **Composition.**

(i) 2ic Bde Sig.

(ii) SO1 G3 Sig(at sig bde level).

(iii) SO1 G3 Ops (Inf).

(iv) Radio det.

(v) Line det.

(vi) Provost section.

(vii) Defense section.

(b) **Function**.

(i) To see that the area selected for the formation HQ is suitable from tactical and comm point of view.

(ii) General distribution of the area for operational and admin purposes.

(iii) Detailed site of the Hq elements.

(iv) Sign posting and leading the layout group.

(2) **Layout Elements.**

(a) **Composition**.

(i) OC RR.

(ii) OC Comcen.

(iii) OC Lines.

(iv) Step up radio switchboard sets for comm. with lower and higher Hqs.

(vi) Step up switchboard.

(vii) Radio relay terminal.

(b) **Functions.**

(i) Movement in advance of the Hq and establish a skeleton Hq before their arrival.

(ii) Provide essential security, command and communication at the new location.

(iii) Determine detailed layout of all remaining elements.

(3) **Rover Group.**

(a) **Composition.**

(i) Bde Comd.

(ii) CO Fd Arty Regt.

(iii) CO Fd Engr Regt.
(iv) Rover sig elements
(v) SO2 G3 (Int).
(vi) Defence Pl.

(b) **Function**. To move close to the adversary and influence the battle.

(4) **Main Hq.**

(a) **Composition.**

(i) Bde HQs staffs.
(ii) Gar Comd.
(iii) G3 plains.
(iv) BALO.
(v) Bde Int Offr.
(vi) LO's.
(vii) Radio, RR, sig and crypto centre.
(viii) Support element and stores.
(viiii) Admin elements.

(b) **Function.** When the Reece group is fully established and has assumed control, the main hq cloes down in the old location and moves forward to the new loc.

(5) **Admin Gp.**

(a) **Composition.**

(i) ST.
(ii) EME.
(iii) Ord.
(iv) Med.
(v) MP Rep.
(vi) Sig Det.

(b) **Function.** The elements of the admin gp are responsible for providing smooth admin and logistics support.

e. **Composition of G3 Cell, G1/G4 Cell and G6 Cell.**

(1) **G3 Cell.** The G3 cell is subdivided into G3 Ops and G3 Sp as follows:

(a) **G3 Ops**.
- (i) SO2 G3 Ops.
- (ii) SO2 G3 Int.
- (iii) Watch keepers.
- (iv) Radio dets.
- (v) Lines det.
- (vi) UAV det.

(b) **G3 Sp**.
- (i) COS.
- (ii) Ba10.
- (iii) OC Pro Coy.
- (iv) Bde Int Offr.
- (v) Los.
- (vi) Radio det.
- (vii) Lines det.
- (viii) G 3 Cell clks.

(2) **G1/G4 Cell.**
- (a) DCOS.
- (b) SO2 G4.
- (c) Radio det.
- (d) Lines det.
- (e) Log sp elms.
- (f) G1/G4 Cell clks.

(3) **G6 Cell.** The G6 cell is subdivided into G6 Main and G6 Support as follows:

(a) **G6 Main.** The G6 Main is responsible for providing

communication for smooth running of the Bde HQs. The G 6 Main is composed as follows:

(i) OC COMCEN.
(ii) Msg centre/Sig centre.
(iii) Crypto det.
(iv) RR det.
(v) DRs.
(vi) SWBD.
(vii) SDS.

(b). **G6 Support.** The G 6 support is responsible for repair and maintenance as well as battery charging workshops and equipment store. The compositions of the G6 Sp include the following:

(i) CO Bde Sig.
(ii) Radio det.
(iii) Lines dets.
(iv) Technical store.
(v) Cook house.
(vi) Officer's mess.
(vii) Battery workshop.
(viii) Maintenance workshop.

f. **Veh Marking for Mov.**

Serial	Gp	Letter	Colour
(a)	(b)	(c)	(d)
1.	Recce	A	Red plate written with black.
2.	Rover Gp	B	Green plate written with black.
3.	Ops Gp	C	Black plate written with white.
4.	Sig Ops	D	Yellow plate written with white.
5.	Admin Gp	E	Blue plate written with black.

e. **Signal Battle Procedure for Movement of Hqs in the Field.**

(1) Receive WngO.
(2) Obtain brief from the Comd/G Staff.
(3) Examine ground/terrain study.
(4) Plan and conduct initial recce.
(5) Issue WngO.
(6) Conduct comm. estimate.
(7) Formulate plan.
(8) Brief Comd/G Staff.
(9) Recce and site loc.
(10) Issue comm. plan.
(11) Monitor situation.
(12) Conduct movement as necessary

f. **Sitting and Layout of Hqs in the Field.** For sitting of Hq in the field, there are tactical and technical consideration as follows:

(1) **Tactical Consideration.** (a) Control of battle.

(b) Communication.

(c) Space.

(d) Defence.

(e) Ground.

(g) Cover from weather.

(h) Concealment.

(i) Low lying areas, nearness to swamps and other health hazards should be avoided as far as possible.

(2) **Technical Considerations.**

(a) The area should provide good HF and VHF radio sites.

(b) Hard standing is necessary for moving in/out of heavy vehicles.

(c) Adequate space for dispersion of radio sets is essential to avoid mutual interference.

(d) Must be within radio communication range of the lower fmns/units.

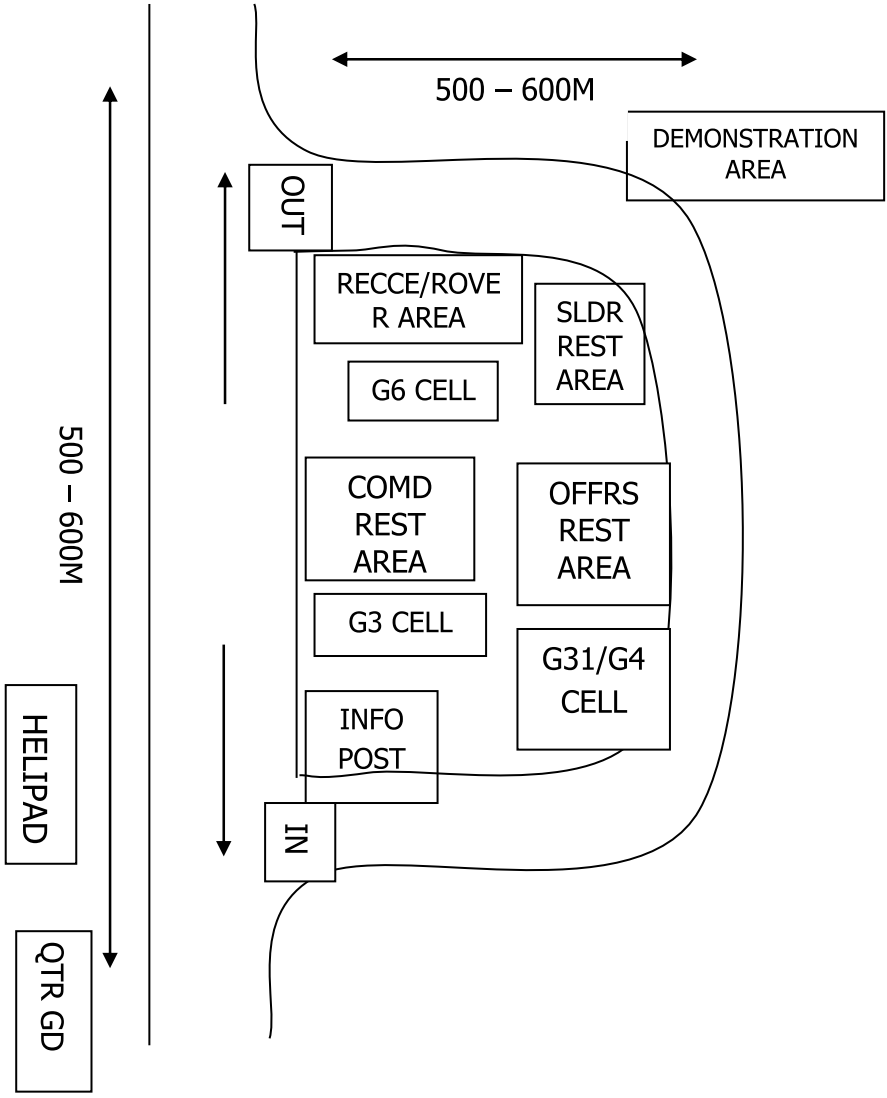
(e) Proximity to existing NITEL lines and other civillian (GSM) comm in the area is desirable if the opportunity is provided.

(f) Availability of electrical power is desirable.

(g) Avoidance of high tension power transmission lines is essential.

(h) Availability of roads and tracks for line laying parties and dispatch service vehicles is desirable.

SKETCH SHOWING A BDE HQ LAYOUT IN THE FIELD



SATELLITE COMMUNICATION

10. Candidates are to be familiar with the following:

a. **What is Communications Satellite**. A communications satellite is an artificial satellite that relays and amplifies radio telecommunications signals via a transponder. it creates a communication channel between a source transmitter and a receiver at different locations on Earth. Communications satellites are used for radio communication, television, telecoms services, radio services, internet, and military applications.

b. **Types of Satellite.**

(1) **Astronomy Satellites.** Astronomy satellites are deployed to observe atmospheric space for the purpose of making star maps, study mysterious happenings, to make map of different planetary surface as well as taking pictures of solar system.

(2) **Atmospheric Studies Satellites.** Atmospheric studies satellites are used to study the characteristics and features of atmosphere.

(3) **Communications Satellites**. Communications satellites are deployed to support communications.

(4) **Navigation Satellites.** Navigation satellites are deployed to support navigation and geo location process.

(5) **Reconnaissance Satellites.** Reconnaissance satellites are used to provide battlefield intelligence and enhancing battle field awareness.

(6) **Remote Sensing Satellites**. Remote sensing satellites are used to detect and classified objects on earth surface, atmosphere and ocean based on propagated signals.

(7) **Space Exploration Satellites.** Space exploration satellites are sent out into deep atmospheric space for further research base on some vital information.

(8) **Weather Satellites**. Weather satellites are used for studying atmospheric weather and climate for the purpose of weather forecast.

c. **Categories of Satellite Communication Services**

(1) **Broadcasting Satellite Services.** Broadcasting Satellite system provides the services for distribution of video and audio streams through satellite. Usually utilize Ku-Band and propagate circular polarization wave pattern.

(2) **Fixed Satellite Services.** The services implement point to point communication and network via satellite between fixed Stations and utilize C-Band and lower power portion of Ku Band spectrum. Very Small Aperture Terminal (VSAT) is an application for fixed satellite services which provide wide area coverage and offers borderless communication within the satellite coverage area.

(3) **Mobile Satellite Services**. The services implement point to point communication and network via satellite between mobile stations. Services are available to the maritime users and land users in any locations. Satellite phone is a type of mobile phone that connects to orbiting satellites instead of terrestrial cell sites.

d. **Satellite Communication Frequency Spectrum.** There are number of radio frequency ranges used in satellite communications. These include S, C, X, Ku, Ka, EHG and V-band. They are given below:

(1) **S Band (2 -4 GHZ).** The S Band is used for

Weather RADAR, surface ship RADAR, and some communications satellites.

(2) **C-Band (4–8 Ghz).** Primarily used for satellite communications and full time satellite TV networks.

(3) **X-Band (8–12 GHZ**). Primarily used by the military. It is also used in RADAR applications, civil, military and government institutions for weather monitoring, air traffic control, maritime vessel traffic control, defence tracking and vehicle speed detection for law enforcement.

(4) **KU-Band (12–18 GHZ).** It is used for satellite communications.

(5) **Ka-Band (26–40 Ghz**). It is used for communications satellites with high-resolution and close-range targeting RADARs on military aircraft.

(6) **EHG (30 -300 GHZ).** It is used for communications satellites.

(7) **V Band (36-51.4 GHZ).** It is used for communications satellites.

e. **Components of Satellite Communications.**

Within the satellite there are two major sections:

(1) **The Bus.** The bus contains the support vehicle and control subsystems that allow the payload to perform its mission. Within the bus, we find:

(a) Tracking eqpt.
(b) Telemetry eqpt.
(c) Ranging eqpt.
(d) Solar panels.
(e) Batteries.
(f) Reaction control system.
(g) Attitude and spacecraft control processing.
(h) Thermal control.

(I) Structure.

(2) **The Payload.** The payload is the business end of the satellite, consisting of the following:

(a) Repeater.
(b) RF multiplexers.
(c) Power amplifiers.
(d) Channel processing and switching.
(e) Transponders.
(f) Antennas.

f. **Advantages and Disadvantages of Satellite Communication.**

(1) **Advantages**.

(a) High bandwidth.
(b) Coverage over a large geographical area.
(c) Can be cheaper over long distances.
(d) High-quality audio and picture display.
(e) Access to hundreds of services worldwide.
(f) The ability to receive and send broadcast signals using satellite technology increases the possibilities of gaining access to channels from other countries that utilize similar technology for broadcasting.
(g) Choice of programs in that a number of unique channel packages are there for the choosing by satellite TV subscribers.
(h) No long transmission delay.
(i) Does not require high power.
(j) Does not require direction antenna.

(2) **Disadvantages**.

(a) Huge initial cost.
(b) Congestion.
(c) Propagation delay.
(d) Can malfunction in bad weather.
(e) Space debris.
(f) Risk of collision.
(g) Low latency.
(h) Wears and tears.
(i) Short life span.
(j) Issue of low coverage.

g. **Applications of Satellite Communication.**

(1) **Broadband Digital Communications**. Broadband satellites transmit high-speed data and video directly for broadband services.

(2) **Direct-Broadcast Services**. Direct broadcast satellites transmit signals for direct reception by the general public, such as satellite television and radio.

(3) **Environmental Monitoring**. Environmental monitoring satellites carry highly sensitive imagers and sounders to monitor the Earth's environment, including the vertical thermal structure of the atmosphere and the movement and formation of clouds.

(4) **Fixed-Satellite Services.** Satellites provide fixed satellite services transmit radio communications between ground Earth stations at fixed locations. Satellite transmitted information is carried in the form of radio-frequency signals. In addition, fixed satellite services satellites provide a wide

variety of services.

(5) **Government.** Nigeria has designed and built satellites which could be available for lease to government users and agencies as well as other friendly and allied nations within the satellites' extensive coverage areas. The NCC used specially allocated frequency bands for freq allotment applications.

(6) **Mobile Satellite Services.** Mobile Satellite Services use a constellation of satellites that provide communications services to mobile and portable wireless devices, such as cellular phones and global positioning systems.

(7) **Navigation and Location.** Personal or car satellite navigation devices are used for point to point navigation, locating distress calls as part of emergency interventions, monitoring coastal and beach erosion, fleet tracking, animal tracking. geo-tagging, fun or educational mobile applications.

(8) **Decision Making Easier**. With more sources of data, from satellite, being more accessible to more people than ever before, the understanding of places and spaces phenomena is potentially better than ever. The services rely on multitude of data sources, algorithms and software to extract only the information which is relevant and necessary to the decision maker, and to present it in a way that is useful –often on digital maps, or colour coded.

(9) **Always Connected**. Satellite phone is used as a back up by formation and units in

the NE who need to ensure continuity of support and reinforcement in any circumstance, particularly when the radio are down. They are the only option for communicating in areas lacking terrestrial infrastructure. The formation and units can carry out vital usage such as make distress calls.

(10) **Military Communication.** It providing robust and sophisticated secure communications network.

(11) **Extracting Mineral Deposits With Remote Sensing Based Spectral Analysis**. During the pre-feasibility and feasibility stages of the mineral exploration, satellites assist determine the mineral potentiality of the area under consideration.

(12) **Providing a Base MAP for Graphical Reference and Assisting Operations Planners and Military Engineers.** The amount of details that produces high resolution satellite imagery is of immense value and provides an extreme amount of detail of the focus and surrounding areas. As maps are location based, aerial imagery supports troops to orient themselves.

(13) **Disaster Mitigation Planning and Recovery**. The result of a natural calamity can be calamitous and at times difficult to assess. But a disaster risk assessment is essential for rescue workers. Object-based image classification using change detection is a quick way to get damage assessments.

Other similar applications using satellite imagery in disaster assessments include measuring shadows from buildings and digital surface models.

(14) **Satellite Communication Can also Provide**:

(a) Long distance education.

(b) Entertainment.

© It could serve civilian in rural area where terrestrial communication network does not exist by providing telephony service.

(d) it provides communication when the terrestrial systems fail due to disaster such as earthquake, volcanic eruption floods, drought, cyclones, landslides and epidemics.

CYBER SECURITY

11. Candidates are to be familiar with the following:

a. **What is Cyber Security**. Cyber security is the practice design to protect network, computer, data and programs against damage or unauthorized access. Cyber security or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide. The elements of cyber security include application security, information security, network security, disaster recovery as well as training and end user education. The cyber security can be make robust through policy, training, commitment in cyber warfare and knowledge among others.

a. **Cyber Definitions**.

(1) **Cyber Terrorism**. Cyber terrorism is the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society. Cyber terrorism is also the use of the Internet to conduct violent acts that result in or threaten the loss of life or significant bodily harm in order to achieve political gains through intimidation.

(2) **Cyber Warfare**. Cyber warfare is the use of computer technology to disrupt the activities of a state or organization. It is also defined as actions by a nation state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.

(3) **Cyber Spying/Espionage.** Cyber spying or cyber espionage is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information, from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious.

(4) **Cyber stalking**. Cyber stalking is the repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails or SMS.

(5) **Cyber Ethics.** Cyber ethics is the philosophic study of ethics pertaining to computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society.

(6) **Cyber Attack**. Cyber-attack is also a type of offensive maneuver employed by individuals or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.

(7) **Cyber Space**. This is a space in which computer transactions occur, particularly transactions between different computers. It is also the online world of computer networks especially the internet.

(8) **Cyber Link.** Cyber Link software applications features media suite which is an allin-one package. Media Suite allows users to watch Blu-ray discs, face-tag photos, edit audio and burn discs among a range of other functions. Its main competitors are Corel Digital. (9) **Cyber Crime**. Cyber-crime is any harmful act committed from or against a computer or network. It is also any illegal behavior directed by means of electronic that targets the security of the computer systems and the data processed by them.

b. **Measures to Achieve Cyber Security**.

(1) When a compromise occurs, the organizations that fare the best will be those that quickly detect the issue and have a plan or measure in place to respond.

(2) Implementing such measures as intrusion detection systems and intrusion prevention systems, anti-virus software can help to detect compromises in their earliest stages.

(3) An effective cyber security response plan will

limit damage, increase the confidence of partners and users, and reduce recovery time and costs.

(4) Plans should include measures for reacting to destructive malware in an Internet Connection Sharing environment.

(5) The need for "manual operations" if network cond tions impact visibility from the Supervisory Control and Data Acquisition System (use for monitoring system, plant or equipment) or if malware potentially renders control devices inoperable via an automated means.

(6) Rather than being developed by a single entity, the plan should be a product of collaboration between all departments that would be stakeholders in a cyber security incident. This will ensure a cooperative and unified response that leverages all of an organization's resources to the greatest extent possible.

(7) For enhanced responsive capability in the event of a cyber-security incident, organizations.

(8) The developed plan or measures needs to be operationalized as well.

(9) It is critical that plans be routinely reviewed and updated to ensure they remain relevant and useable for when they are actually needed.

(10) Furthermore, to truly understand cyber security incident response plan, organizations must practice them through regular exercises. This will ensure that all stakeholders understand the procedures that would be implemented in the event of a significant cyber disruption or breach, enabling a

more effective and efficient response.

(11) Plan and measures should include Malware Threats and Mitigation Strategies.

(12) There will be need to also developing an Internet Connection Sharing Cyber-security Incident Response Capability.

(13) The need for backup of the critical information and data base.

(14) Authenticate network users.

(15) The use of password security.

(16) There will be need for enhance physical security of hardware and software.

(17) There will be need for adequate capacity building in area of cyber -security.

UNMANNED AERIAL VEHICLES

12. Candidates are to be familiar with the following:

a. **What is a UAVs.** Unmanned Arial Vehicle is an aircraft with no pilot on board which can be remotely controlled or fly automatically based on preprogrammed flight plans or more complex dynamic automation system. Modern UAVs systems are capable of acquiring intelligence and carrying out recce and surveillance.

b. **Types of UAVs**.

(1) **Combat UAVs**. Providing attack capability for high risk missions.

(2) **Logistic UAVs**. Delivering cargo.

(3) **Target and Decoy UAVs**. Providing ground and aerial gunnery a target that simulates an enemy aircraft or missile.

(4) **R and DUAVs.** Improve UAV technologies.

(5) **Reconnaissance UAVs**. Providing battlefield intelligence.

(6) **Civil and Commercial UAVs.** Agriculture, aerial photography, data collection.

c. **Classification of UAVs.** UAVs can be classified from medium to large system as well as small system.

(1) **Medium to Large System UAVs.** The medium to large system of UVA's range from dozens of kilograms to the sizes of a manned planned. They can fly at high or medium altitude for hours or days at a time, hundreds or thousands of miles from their operators.

(2) **Small systems (mini and micro UAVs).** Small systems are small enough to be carried by or two people. These systems are generally limited for a few kilometers and short flight time.

d. **Components of UAVs.**

(1) Auto Pilot.
(2) Radio control.
(3) Ground Control Station.
(4) Pay load (camera and weapon system).
(5) Body.
(6) Power platform.
(7) Computing.
(8) Actuation.
(10) Software.
(12) Flight control

e. **Features of UAVs**.

(1) They can easily fly even when in strong wind conditions.

(2) The frame or the main components are made of carbon fiber, which is widely used in aerospace industry for its characteristics such as:

Physical strength, robustness and light weight.

(3) Safe and easy flight operations.

(4) Emergency fail safe recovery.

(5) Flight data recording.

(6) Redundant flight control system.

(7) Low-stress and panic free flying.

(8) Advanced Global Positioning System.

(9) Voice announcement and loggings of the telemetry data.

(10) Telemetry on PC or tablet.

(11) Carrying sensitive videography and monitoring equipment.

(12) UAV uses electric batteries and battery recharging station.

(13) Rapidly deploy with simple controls and quick-snap power allows for rapid deployment with full autopilot with a simple remote control.

(14) Advance navigation system that allows pilots the ability to complete fully autonomous missions.

(15) The GPS monitoring systems and integrated Autopilot offers the ultimate in safety with the 'Home' mode. If the UAV lose power and becomes out of range for any reason, the UAV returns to a pre-determined GPS point, hovers for 1 minute and then auto-lands and shuts down all rotors.

(16) Unbeaten fuel consumption figures.

(17) Shorter take-off and landing distances.

(18) Rapid climbs to altitude.

(19) Faster transits to and from station.

f. **Challenges Facing the Deployment of UAVs.**

(1) Inadequate platform.

(2) Lack of integration and ground station.
(3) Inadequate training.
(4) Poor funding.
(5) Inadequate maintenance system.

g. **Strategies to Sustain the Uses of UAVs in NA.**

(1) Need to acquire more platforms.
(2) The need to integrate the UAV training unit.
(3) Effective and efficient training.
(4) Adequate funding.
(5) Smart Communication platform systems.
(6) The need for collaboration with other agencies

h. **Applications of UAV**.

(1) **Military Applications.**

(a) The reconnaissance UAVs is intended for reconnaissance to a depth of several hundred kilometers from the front line at supersonic speeds.

(b) A supersonic long range reconnaissance UAVs are intended for conducting aerial photographic.

(c) A long range reconnaissance UAVs are use for conducting signals intelligence to a distance location.

(d) UAVs providing mission intelligence for ops planning.

(e) UAVs armed with missiles have been used as platforms for hitting ground targets, mostly aimed at assassinating high profile individuals (terrorist leaders, etc.).

(f) UAVs are used for combat training of

human pilot.

(g) UAVs with advanced imaging technology configure with map can be used for clearing of minefields.

(h) UAVs can also perform flyovers and gather images at various wavelengths which could indicate explosive chemicals seeping from landmines into the surrounding foliage.

(i) The unmanned airborne de-mining system can uses a three step process to autonomously map, detect and detonate land mines.

(j) Military search and rescue ops.

(k) Inspection of power lines and pipelines by tps on duty.

(l)Delivering logs supplies to tps in an inaccessible regions.

(m) Cooperative environment monitoring in jtops.

(n) Border patrol missions.

(o) Convoy protection.

(p) Coordinating humanitarian aid.

(q) Crowd monitoring for IS.

® UAVs in commercial aerial surveillance is expanding with the advent of automated object detection.

(s) UAVs can help in disaster relief by providing intelligence across an affected area.

(t) UAVs as part of a system to survey and monitor pipelines, dams and other rural infrastructure in support of the military assistance.

(u) UAVs equipped with air quality monitors provide real time air analysis at various elevation.

(2) **Civil Applications**.

(a) Civil uses of UAVs include aerial crop surveys. UAVs are now becoming an invaluable tool by farmers in other aspect of farming, such as monitoring livestock, crops, water levels, crop spraying, as they are often cheaper than a full-sized helicopter for the purpose.

(b) Home security, road patrol, antipiracy

(c) Delivering medical supplies to otherwise inaccessible regions.

(d) UAVs are used for counting wildlife, surveillance applications include livestock monitoring and wildfire mapping and detection of illegal hunting.

(e) Forest fire detection and monitoring.

(f) Coordinating humanitarian aid.

(g) Large-accident investigation.

(h) Landslide measurement.

(i) Illegal landfill detection.

(j) Crowd monitoring in support of election.

(k) Private citizens and media organizations use UAVs for surveillance, recreation, news-gathering, or personal land assessment.

(l) An animal rights group used UAVs to film hunters shooting wildlife.

(m) UAVs are used for commercial and motion picture film-making

(n) Law enforcement departments used UAVs for law and order and aerial surveillance.

(o) UAVs were used in search and rescue after hurricane and help in disaster relief by providing intelligence across an affected area.

CLOSE CIRCUIT TELEVISION

13. Candidates are to be familiar with the following:

a. **What is a CCTV.** The CCTVis the abbreviation for closed circuit television. It is a system that sends television signals to a limited number of screens, and is often used in public places to prevent crime. CCTV is also known as video surveillance. It involved the use of video cameras to transmit a signal to a specific place, on a limited set of monitors for surveillance and security purposes. The CCTV Surveillance System is very important for security of our valuable assets (KPs and Vps). The CCTV can be use to monitor premises and prevent misuse of resources or track lazy personnel. In case of any incident you can easily extract the recordings from digital video recorder and use it for investigations.

b. **The Components of CCTV**.

(1) Radio.
(2) Cables.
(3) Digital Video Recorder.
(4) Power Supply System.

c. **Types of CCTV Camera**.

(1) Bullet.
(2) Ceiling Mount.

(3) Day/Night Vision.
(4) Wireless.
(5) HD camera.
(6) Thermal Image.

d. **Types of Network/IP Surveillance Cameras.**
(1) Fixed.
(2) Fixed Dome.
(3) Pan Tilt Zoom Camera(PTZ).
(4) A PTZ dome camera.
(5) Non Mechanical Pan Tilt Zoom.

e. **Feature of Network/IP Surveillance Cameras.**
(1) **Auto Focus.** The auto focus features of Network/IP Surveillance cameras that can be zoomed could be handy when working with PTZ IP Cameras.
(2) **Night Vision.** Many Network/IP Surveillance cameras support night vision which makes the image viewable at night, in black and white.
(3) **White Balance.** Some Network/IP Surveillance cameras can identify the light source used and compensate for its colour which is useful to reflect the natural colours.
(4) **Bandwidth Limiting.** Certain Network/IP Surveillance cameras can limit the bit rate at which the images are sent via the network and hence controlling the network bandwidth that is required to transmit the captured video image of the IP Cameras.
(5) **Freeze.** Images can be freezed during the pan, tilt and zoom operation (for PTZ Camera) and the current image can be shown after the camera has

reached its position.

(6) **Back-light Compensation.** The feature makes the focused objects look more clear against a bright background.

(7) **Audio**. Some Network/IP Cameras allows for recording the voice along with video.

(8) **Camera Preset Positions**. Many Network/IPSurveillance cameras allow for setting preset camera viewing angle/zoom positions which can also move through the selected preset positions in set order or at random.

(9) **360 Degree View**. Certain PTZ cameras support continuous 360 degree rotation for coverage.

(10) **Motion Detection**. This feature is used to generate an alarm wherever movement occurs in the image.

(11) **Interchangeable Components**. Some Network/IP Surveillance cameras provide interchangeable components (including the CPU, power supply, cameras etc) and individuals components can be replaced/changed at any time. This help rectify fault.

(12) **Analog Connectivity**. Some Network/IP Surveillance cameras come with an optional analog connectivity which can also connect to the co-axial cable network in addition to the IP network. Analog surveillance cameras can be connected to the IP network using Video encoders.

(13) **Privacy Marks.** Network/IP Surveillance cameras allows to block/blur certain parts of the screen using privacy masks. In some IP Cameras,

these privacy masks increase their size automatically.

(14) **Recorded Tour**. Some Network/IP Cameras allows the recording of the movements of the operator and the same can be played back later.

(15) **Alarms**. If any unwanted incidents happen with the cameras like cutting the cables etc, that can stop the functioning of the IP cameras, certain alarms can be activated by them based on the event and severity. These alarms can range from sending emails or SMS to activating an external device automatically through input/output port available in the cameras.

(16) **Simultaneous Streaming of Multiple Formats**. Certain Network/IP Surveillance cameras support the streaming of multiple compression formats.

(17) **Auto-tracking**. Some Network/IP Cameras support auto-tracking of images where Pan and Tilt can be automatically controlled the camera to follow moving objects by centering them in the screen.

(18) **Power Over Ethernet**. Many Network/IP Surveillance cameras support power over Ethernet feature which lets the network data cable to carry both power and data simultaneously without having to carry a separate power cable to the cameras.

(19) **Wireless**. Some Network/IP surveillance cameras support wireless connectivity to networks/access points.

(20) **Application Programming Interface.** Some Network/IP Surveillance cameras give an open standards based Application Programming Interface that enables many software vendors to write programs for specific applications using the Network/IP cameras.

f. **Applications of CCTV**.

(1) In industrial plants, CCTV equipment may be used to observe parts of a process from a central control room.

(2) CCTV systems may operate continuously to monitor a particular event.

(3) A more advanced form of CCTV, utilizing digital video recorders that provides recording for many days with a variety of quality and performance options and extra features.

(4) A camera mounted at the entrance to an area will enable you to monitor and record all vehicles, with their number plates, twenty-four hours a day. This is used at a number of locations to deter armed robbery and undesirables from entering.

(5) It can be used to adequately cover car parks to cover a large area on a continuous basis and allow the CCTV operator to zoom into recordings and view faces and after the event has happened.

(6) A target for the criminal element can be adequately protected by the use of CCTV.

(7) At receptionists, installed cameras on some sites give a clear view of everyone standing at the counter. This not only gives a visual record of people as they arrive on site but also acts as a deterrent to criminal or abusive behaviour.

(8) A camera placed within an ops room, COMCEN or offices to deter unauthorised staff entry, while a camera outside the can give the staff inside a view not only of who is opposite the door but also anyone else in the general area.

(9)It can be used to detect unauthorised visitors entering the restricted area and to make sure that

personnel are doing their job and not simply congregating at a single point for a chat.

(10) Cameras can also be used on your behalf to ensure that safety policy is adhered to in areas that cannot be directly observed.

(11) CCTV Increase your employees Productivity

(12) CCTV Increase your ability to efficiently manage your business

(13) CCTV image of an incident can be far more useful than a mere verbal description of a suspect by a witness.

(15) Other applications include:

(a) Traffic Monitoring.
(b) Sporting Events.
(c) Use in Schools.
(d) Training Purpose.

DOCUMENTS REQUIRED FOR COMM PLANNING

14. Candidates are to be familiar with how to prepare the following:

a. Communication Estimate.
b. Communication Plan.
c. Preliminary Instructions.
d. Movement Order for moving a bde hq in the field.
e. Communication Electronic Instructions.
f. Recce plan.
g. Recce report.
h. Task org.
i. Sig OpO.
j. Comm contingency plan.
k. Sig IPB/PPA.
l. SOP relevant extraction.
m. Admin/tecnical instruction.

RADAR SYSTEM

15. Candidates are to be familiar with the following:

a. **What is a RADAR**. The word "RADAR" is an acronym derived from the words Radio Detection and Ranging. RADAR is an object detection system that uses radio waves to determine the range, angle, or velocity of objects. It work base on the technique of using radio waves to detect the presence of objects in the atmosphere. RADAR was designed shortly before World War II. Today, RADAR is used for a wide array of applications such as detecting the presence, direction, distance, and speed of tank, aircraft, ships, and other objects by sending out pulses of high frequency electromagnetic waves that are reflected off the object back to the source. A RADAR system consists of the following components: transmitter, receiver, antenna and processor.

a. **Components of RADAR System**. A radar system consists of the following component:

(1) **Transmitter**. The transmitter producing electromagnetic waves in the radio or microwaves domain.

(2) **Antenna**. The antenna is used for transmitting and receiving electromagnetic waves signals.

(3) **Receiver.** The receiver received the electromagnetic waves in the radio or microwaves domain from the transmitter.

(4) **Processor**. The processor determine the properties of the objects thereby giving information about the object's location, direction and speed.

b. **Types of RADAR System**. The two major types of RADARs are primary and secondary RADARs. While the primary radar work on basis of detecting echo of

radio waves transmitted by earth station, the secondary radar depends on signal from transponders onboard the aircraft. The primary and secondary RADARs can be further subdivided into the following:

(1) **Nautical Radars**. Nautical RADARs is used to locate landmarks and other ships in ocean. It is also used as ocean surveillance systems.

(2) **Aviation Radars**. Aircrafts are equipped with Aviation RADAR devices that warn of obstacles in approaching their path and give accurate altitude readings.

(3) **Marine Radars**. Marine radars are used to measure the bearing and distance of ships to prevent collision with other ships and navigation purposes.

(4) **Weather-Sensing Radars**. Weather Sensing RADARs is an important tool in weather forecasting and helps make the forecasts more accurate.

(5) **Detection and Search Radar**. Detection and search radar is the "early warning RADAR", which is used for longrange detection of objects.

(6) **Target Acquisition Radar systems**. Target acquisition radar systems is used to locate surface to air missiles. These types of RADAR are often used in the military and in coastal surveillance, as well as for detecting car speed in high way patrol.

(7) **Missile Guidance Systems**. Missile guidance systems is used to locate the target of missile often present in Military aircraft.

(8) **Radar for Biological Research**. Bird and Insect RADAR are used frequently by scientists to track the migration patterns of animals.

(9) **Air Traffic Control and Navigation Radar.** Air traffic control and navigation radar is used by airport to ensure the safety of planes. This type of RADAR detects the proximity of an aircraft and identifies the identity and altitude of the plane.

(10) **Doppler Radar.** Doppler RADAR is used for measuring wind direction and speed by measuring the Doppler effect. The RADAR also measures what is called radial velocity.

(11) **Weather radars**. Weather RADARs are used to measure wind speeds and dual polarization for identification of types of precipitations.

(12) **Navigational Radars**. The Navigational RADARs resemble search RADAR, but use very short waves that reflect from earth and stone. They are common on commercial ships and long distance commercial aircraft.

c. **Applications of RADAR System**. The Applications of RADAR System include the following:

(1) The first use of radar was for military purposes to locate air, ground and sea targets.

(2) Aircraft are equipped with RADAR devices that warn of aircraft or other obstacles in approaching their path, display weather information, and give accurate altitude readings.

(3) Marine RADARs are used to measure the bearing and distance of ships to prevent collision with other ships.

(4) It assist to navigate and to fix ship position at sea when within range of shore or other fixed references such as islands, buoys, and lightships.

(5) In port or in harbour, vessel traffic service RADAR systems are used to monitor and regulate ship movements in busy waters.

(6) Meteorologists use RADAR to monitor precipitation and wind. It has become the primary tool for short-term weather forecasting and watching for severe weather such as thunderstorms, and, winter storms.

(7) Geologists use specialized ground penetrating RADARs to map the composition of Earth's crust.

(8) Police forces use RADAR to monitor vehicle speeds on the roads.

(9) Ground penetrating RADAR data on the subsurface of volcanic, icy and arid terrains are key elements in understanding the geological evolution of Earth's subsurface.

(10) **Cloud Radar Applications.** This is used to detect and help estimate snowfall and light rain.

(11) **Scatterometry Applications.** This is used to map the horizontal wind vector field over Earth's oceans, the surface cross-sections that are measured by this instrument have many other applications, including the identification and mapping of different classes of sea ice, ranging from older and thinner seasonal ice.

(12) **Radar Ecology Applications**. This is capable of detecting forest fires and planning for fire management. RADAR sensors from airborne or space borne platforms have the potential of providing quantitative information about the forest structure and biomass components that can be readily translated to meaningful fuel load estimates for fire management.

(13) **Ocean Vector Winds Applications**. This application produces estimates of the near surface horizontal wind speed and direction over the ocean.

(14) **Radar Interferometry system**. This application is used to produce highly accurate topographic map.

NA ICT Policy 2016

16. Candidates are to be familiar with NA ICT Policy 2016.

NAWANI

17. Candidates are to be familiar with the following:

a. **What is NAWANI**. NAWANI was meant to provide specialized ICT facilities applications and solution for the NA. The ultimate objective of the NAWANI project was to transform the NA into centric force like any other modern day IT driven army. The objective of the NA ICT Policy is to use ICT as a major tool to engineer and transform the NA into a more effective, efficient and knowledge based fighting force. In order to achieve this objective, the AHQ DAPP is responsible for the approval and implementation of all ICT policies in the NA after formulation by HQ NAS and the consent of COAS. NAWANI is therefore the flagship of military comm eqpt since it integrated into various services.

b. **Current State of NAWANI**. The NAWANI was meant to provide specialized ICT facilities application and solution. The services and facilities currently available in NAWANI include:

(1) Virtual Private Network.
(2) Internet.
(3) Email Services.

(4) Video Conferencing.
(5) Data Centre.
(6) Human Resources Mgt System.
(7) Payroll Applications.
(8) Biometric Enrolment System.
(9) Dynamic Archiving.
(10) Disaster Recovery.
(11) System Applications.
(12) Produc Software.

c. **NAWANI Infrastructures.**

(1) VSAT (2) Computers.
(3) Scanners.
(4) Routers.
(5) Gate.
(6) Switch.
(7) Hub.
(8) Optic Fabre.
(9) Cables.
(10) Video Card.
(11) Terminals.
(12) IP Phone.
(13) Operation Software.

d. **How to Achieve Operational Efficiency and Reliability of NAWANI.**

(1) Enhancing the composition of the infrastructures.
(2) The used of efficient and effective types of infrastructure.
(3) Good configuration of the infrastructure.
(4) Suitable HW and SW.
(5) Enhance Bandwidth.

(6) Robust video and video data solution.
(7) Network compatibility.
(8) Spare part support.

e. **Challenges of NAWANI**.

(1) Inappropriate implementation policy.
(2) Inadequate institutional frame work.
(3) Inadequate Infrastructures.
(4) Inadequate human capacity.
(5) Paucity of funds..
(6) Inadequate sensitization of NA personnel as regard to NAWANI.
(7) Network access control and security.
(8) Change Mgt, in that NAWANI is facing the problem of acceptability by NA personnel.
(9) Non activation of NAWANI address by some fmns/units.
(10) Technical issue in terms of:
  (a) Bandwidth inadequacy.
  (b) Deployment.
  (c) Epileptic internet services.
  (d) Poor Infrastructure design.
  (e) Inefficient power back up.

f. **Strategies to Combat the Challenges Faced by NAWANI.**

(1) Establishment of NAWANI institutional framework with NAS at the centre stage.
(2) Creation of appropriate NAWANI infrastructures.
(3) Human capacity development.
(4) Institutionalization of NAWANI funding.
(5) Sensitization of NA personnel at all level with

regard to NAWANI.

(6) Training to improving the use of current of NAWANI applications.

(7) The need to complete pending work in the inventory mgt syst. and other applications. (8) Expansion and improvement of IP Phone.

(9) Expansion of WAN at Bde and Bn level to enhance usage.

(10) Installation of infrastructures that will enhance NAWANI services.

MILITARY TECHNOLOGY
(INTELLIGENCE)

MILITARY TECHNOLOGY INTELLIGENCE

INTRODUCTION

1. This module is designed to serve as study guide for NAIC candidates writing the Captain to Major Written Promotion Examination (CMWPE). Rather than concentrate on improvement in the science of intelligence, the guide emphasizes practical application of knowledge and experience as practiced in the NAIC today. The CMWPE for NAIC officers is quite comprehensive and covers subjects taught at the YOC Intelligence and predominantly Tactical Intelligence Officers Course. In addition to questions based on the module, they would be others on routine procedures in a typical NAIC unit. No aspect of the module should be treated in isolation as comprehensive knowledge of the subjects is expected to be exhibited. Questions in the examination will combine the 3 parts as the module is only to delineate study areas.

2. Candidates would not be asked yes or no multiple choice type of questions. They would also not be asked questions that would make them reproduce précis. The experience of the candidate at this stage of their career should encompass service knowledge in any of the specialist commands or NAIS and in an Intelligence Regiment or Intelligence Brigade Headquarters. Officers are therefore expected to be fairly widely read to appreciate the expectations of this special to corps examination. The module is divided into 5 broad areas: definitions, principles of intelligence, operational, security and technical intelligence. Definition of terminologies is however not exhaustive in this module and students are required to familiarise themselves with other commonly used intelligence terms.

AIM

3. The aim of this module is to enhance candidates' preparation for the NAIC special to corps paper at the SSCQE.

TERMINOLOGIES AND PRINCIPLES OF INTELLIGENCE DEFINITION OF TERMINOLOGIES

4. **Information**. Unevaluated material of every description, including those derived from observation, reports, rumors, imagery and other sources which when processed, may produce intelligence.

5. **Intelligence**. The product resulting from the processing of information, it may concern foreign nations, hostile or potential hostile forces or elements, or areas of actual or potential operations.

6. **Basic Intelligence**. Intelligence on any subject which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject.

7. **Combat Intelligence**. That knowledge of the enemy, weather and geographical features required by a commander in the planning and conduct of combat operations.

8. **Current intelligence**. Intelligence which reflects the current situation at either strategic or tactical level.

9. **Tactical Intelligence**. Intelligence required by a commander and his staff for the planning and conduct of tactical operations.

10. **Strategic intelligence**. Intelligence required for the determination of national or multi-national policy, and of plans concerning the conduct of operations at strategic level.

11. **Intelligence Requirement**. Any subject, general or specific, upon which there is a need for the collection of information for the production of intelligence.

12. **Information Requirement**. Those items of information

regarding the enemy and his environment, which need to be collected and processed in order to meet the intelligence requirements of a commander.

13. **Area of Intelligence Interest**. That area which a commander requires intelligence on those factors and developments likely to affect the outcome of his current or future operations.

14. **Area of Intelligence Responsibility**. An area allocated to a commander at any level in which he is responsible for intelligence affecting the operations of his command or his commitments to higher command.

15. **Sources**. Anyone or anything from which information can be obtained for intelligence purpose.

16. **Agency**. Any organization or individual engaged in collecting or processing information for intelligence purpose

17. **Collection**. The exploitation of sources by collection agencies and delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.

18. **Signature Equipment**. Any item or equipment that reveals the identity, type or nature of the unit or formation to which it belongs.

19. **Evaluation**. A standardized method of appraisal designed to indicate the degree of confidence that may be placed in any item of information that has been obtained. It usually concerns the system of rating to the reliability of the source and the credibility of the information when both are examined in the light of knowledge available.

20. **Indicator**. Any item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action.

21. **Compromise**. A term normally applied to
classified matter, the unauthorized knowledge of which will constitute a threat to the overall security efforts.

22. **Espionage**. The covert means by which countries,

organizations and individuals acquire or attempt to acquire information concerning the national interest to which they are not entitled.

23. **Subversion**. An action including illegal action, aimed at undermining the authority and strength of a legal government and the loyalty of citizens in order to further the interest of a foreign power or subversive organization.

24. **Sabotage**. Act (excluding normal military operation) or an omission calculated to cause physical damage in the interest of any foreign power or subversive political organization, this does not include malicious damage done in the interest of an individual.

25. **Counter Intelligence**. That aspect of intelligence covering the activity devoted to destroying the effectiveness of Hostile Intelligence Service's (HIS) activities and the protection of information against espionage, personnel against subversion and installation or material against sabotage.

26. **Clandestine**. By stealth, the activity is concealed but not disguised.

27. **Covert**. Activity that is disguised so that its true nature cannot be discovered and leaving no sign of entry- same as surreptitious.

28. **Overt**. Refers to any disguised act whereby information of intelligence value or interest is obtained from an open source.

29. **Talent Spotters**. Links in the HIS chain whose aim is to pinpoint or identify likely subjects who might be susceptible to HIS approach for recruitment.

30. **Brainwashing**. Cleansing of the mind of an established idea by means of persistent psychological pressure.

31. **Indoctrination**. Imbuing the mind with doctrine, idea or opinion.

32. **Stool Pigeons**. Using a plant or traitor among prisoners.

33. **Cut-Out**. A person interposed between 2 communication

links or between one espionage network and another.

34. **Elicitation**. The acquisition of intelligence from a person or group without their being conscious of the intent of the person they are interacting with.

35. **Mole**. Usually a high level agent who is hidden within enemy organization and normally tasked only rarely to furnish extremely valuable intelligence.

36. **Double agent**. A person engaged in espionage for 2 or more intelligence agencies who provides information to one agency about the other, or about each agency to the other.

PRINCIPLES OF INTELLIGENCE

34. The organization, activities and the production of intelligence are governed by basic principles outlined below (CSO ACTS R).

351. **Centralised Control**. Intelligence must be centrally controlled to avoid duplication, provide mutual support and ensure efficiency and economic use of resources.

36. **Systemic Exploitation**. Sources and agencies must be systematically exploited by methodical planning based on thorough knowledge of their capabilities and limitations.

37. **Objectivity**. Any temptation to distort information to fit pre-conceived ideas must be resisted.

38. **Accessibility**. Information and intelligence must be readily accessible since the essence of intelligence processing is comparison. Collation systems must be designed on this principles.

38. **Continuous Review**. Intelligence forecast must be continuously reviewed, and where necessary revised, taking into account all new information and comparing it with what is already known

39. **Timeliness**. Information or intelligence is useless if it arrives too late. Information and intelligence must be disseminated to those who need it and in the most appropriate form as soon as they are

required.

40. **Source Protection**. All sources of information must be adequately protected. Indiscriminate dissemination may endanger a source or agency. Therefore, all information must be disseminated on a need to know basis.

41. **Responsiveness**. Intelligence staff must be responsive to the need of the commander.

OPERATIONAL INTELLIGENCE

42. At the level of Commanding Officer and below, the NAIC officer is expected to know all the resources available to him. In combat situations, he is to make use of the intelligence available to him before commencement of hostilities ie, intelligence from above and information from flanking and subordinate units. Ideally before a commander writes his Operation Orders, the intelligence picture should be available to him. Knowledge of operational issues that contributes to the success of commanders' missions as enumerated below are essential for an intelligence officer.

INTELLIGENCE CYCLE

43. Candidates are expected to be familiar with the intelligence cycle which starts with direction from the commander. Particular emphasis should be placed on
collection and the exploitation of various sources available to an intelligence officer. It is also important to know the intelligence processing and dissemination methods.

44. **Direction**. The commander will direct his intelligence staff and give them clear instructions on the information or intelligence he needs. It involves determining the intelligence requirement, preparing a collection plan, tasking sources and agencies and

checking productivity.

a. **Collection Planning**. The aim of collection planning is to ensure:

(1) That the most suitable source or agency is tasked to collect a particular piece of information.

(2) That tasking of sources and agencies and the result of their collection are collated in an understanding format.

(3) Ease of further tasking and re-tasking where necessary.

b. **Making a Collection Plan**. A formal collection plan must:

(1) Show clearly the critical and other information requirement and the specific questions arising from them which are to be put to the colleting agencies.

(2) Include all sources and agencies.

(3) Indicate which sources and agencies are to be tasked.

(4) Specify the form in which they are to report and the time by which a report is required.

(5) Show how the burden of collection has been spread.

(6) Denotes what information has or has not been collected so that the available effort may be properly re-allocated.

c. **Checking Productivity**. The simplest form of checking productivity is the collection worksheet (See Annex C) or at the higher levels, the maintenance of a record which shows the sources and agencies tasked and the results. The

checking of productivity embraces the intelligence principle of continuous review and also for an essential part of the intelligence cycle.

45. **Collection**. Collection has been earlier defined. In addition, it will be necessary for the student to study some important elements in the collection process.

a. **Sources of Information**. Common sources of information for intelligence purposes include but not limited to the following

(1) Pws.
(2) Local residents.
(3) Refugees.
(4) Captured Enemy equipment and material.
(5) Enemy electro-magnetic emissions and sources.
(6) Drone.
(7) Imagery.
(8) Maps.
(9) Patrols.
(10). Int Rep from BHQ.
(11) Fwd tps.
(12) Sp arms esp arty.

b. **Exploitation of sources and Agencies**. Intelligence Staff must have a detailed knowledge of the capabilities and limitation of all sources and agencies available to them. The selection and tasking of sources will depend on the following factors.

(1) **Security**. Steps must be taken to ensure that

sources and agencies are protected, and so can continue to operate.

(2) **Reliability**. Sources and agencies must have the basic knowledge or technical ability needed to enable them report accurately. Reliability will generally be established by the standard of performance achieved over a period of time.

(3) **Suitability**. A ground patrol should not normally be sent on a task better performed by an aircraft.

(4) **Risk**. In some circumstances, the use of certain sources of information may be physically hazardous to those employed on the mission, or there may be a degree of political risk to the government, country or agency concerned. Any such risk must be measured against the value of the information sought.

46. **Processing**. Processing is condensed into 3 related activities; Collation, Evaluation and Interpretation.

a. **Collation**. This is the procedure for receiving, sorting and recording all reports arriving in an intelligence office at any level. It involves:

(1) The routing office work of registering and recording all incoming information.

(2) Logging Map or chart marking and filing.

(3) The recording of all information in a system so designed that intelligence staff can operate it rapidly and efficiently in condition of stress; recording or retrieving any item without difficulty.

b. **Evaluation**. Evaluation is the appraisal of an item of information in terms of pertinence, reliability, credibility and accuracy. It is part of a trained intelligence officer's virtually instantaneous mental reaction to each piece of information

he receives. If and when he receives information obviously irrelevant to his information requirement, he should automatically log it and at once pass it on to the unit or formation whose area of interest it concerns.

c. **Order of Battle**. Order of Battle (ORBAT) consist of evaluated information regarding any military force. In operations other than war, insurgent forces or underground elements will be included. It usually contains the following elements:

(1) Composition of a unit including identification and organisation.

(2) Disposition including geographical location, tactical deployment and movement.

(3) Strength of personnel, weapons and equipment and type of units.

(4) Tactical status of individual, units and special training.

(5) Tactical doctrine and special operations.

(6) Logistic system and current status.

(7) Combat effectiveness, experience, morale and other code names and numbers.

(8) Personalities, unit history, uniforms and insignia, code names and numbers.

d. **The Grading System**. It is unlikely that intelligence officers will be called upon to grade the reports they sent in, but if they receive graded reports they must be able to interpret the grading. The grading system has been standardised such that degrees of reliability are expressed by the letters A-F and degrees of accuracy by the numbers 1 to 6. Each combination of letter and number forms a grading expressed as follows:

Reliability of Source	Accuracy of Information
A- Completely reliable	1- Confirmed by other Sources
B- Usually reliable	2- Confirmed in part by other. Therefore probably true
C- Fairly reliable	3- Complies with behavioural pattern. Possibly true
D- Not usually reliable	4- Unconfirmed and contradicts estimate. Doubtful
E- Unreliable	5- Unconfirmed and contradicts experience. Improbable.
F- Reliability cannot be judged	6- Truth cannot be judged

47. **Dissemination**. This is the timely conveyance of intelligence in an appropriate form and by any suitable means to those who need it. While dissemination could be done orally or in written forms, the manner and form of dissemination are governed by some principles

a. **Principles**. The principles of dissemination include the following:

(1) Timeliness- To ensure intelligence is received on time.

(2) Accuracy - Facts are to be checked carefully.

(3) Brevity - Brief as possible to prevent uninteresting lengthy reading.

(4) Interpretation - Facts are to be interpreted before dissemination.

(5) Standardisation - To be in logical standardised

sequence.

(6) Distribution - Ensure intelligence staff in area of intelligence interest is informed.

(7) Regularity- Urgent issues are not to be left for regular routine reporting.

(8) Security- Appropriate security classification and strict 'need to know' basis are to be ensured.

b. **Types of Dissemination**:

(1) **Oral Dissemination**. Oral dissemination include:

(a) Impromptu - To meet immediate need of commander or visitor.

(b) Formal – Needs proper preparation and presentation.

(2) **Written Dissemination**. Written dissemination include:

(a) SITREP - A G3 report at regular intervals with 'enemy' paragraph written by intelligence staff.

(b) INTREP - Used to disseminate immediate intelligence, with or without comment which cannot wait for next routine report

(c) INTSUM - Report originated at regular laid down interval with summary of important intelligence within the period.

(d) SUPINTREP - Detail report originated as and when necessary to meet a special situation.

(e) PICTINSUM - A pictorial form of dissemination where reproduction facilities exist.

(f) PRETECHREP – A report warning of the capture or discovery of enemy equipment of intelligence value.

OPERATION SECURITY

48. **Operation Security**. Operation security (OPSEC) includes the application of tactics and techniques to prevent the enemy from gaining knowledge of planned, on-going, or completed military operations or activities. It comprises a number of elements including physical security, information security, signal security etc.

49. **Physical security**. This encompasses the use of security forces, barriers, and other measures to safeguard personnel; to prevent unauthorised access to equipment, facilities, materials and documents and to provide safeguard against espionage, sabotage, damage and theft.

50. **Information Security**. This involves evaluation and when appropriate, the protection of material that if possessed by hostile agencies, might produce intelligence. Eg orders, reports, spoken disclosures and proposed releases to news media.

51. **Signal Security**. Signal Security (SIGSEC) include Communication Security (COMSEC) and Electronic Security (ELSEC). They collectively comprise all measures taken to deny unauthorised persons information of value from telecommunication sources and protection resulting from measures to deny unauthorised persons information of value that may be derived from electromagnetic and non-data related radiation.

52. **Counter Surveillance and Deception Activities**. This include all active and passive measures taken to prevent hostile

surveillance of a force area or base. Eg use of camouflage pattern painting, screen smokes or aerosols, visual disrupters, minimise the possibility of defection and/or identification of troops, materials equipment and installations. Deception include tactical or strategic feints, demonstrations and ruses plus the use of dummy equipments.

53. **Intelligence**. OPSEC and intelligence are separate but constantly supporting activities thus related aspects of each should be closely coordinated. A successful OPSEC programme rests upon an understanding of the enemy intelligence efforts.

54. **Counter Intelligence**. Counter intelligence (CI) traditionally supports OPSEC by destroying the effectiveness of inimical foreign intelligence activities and protecting information against espionage, individuals against subversion and installations or material against sabotage.

55. **Electronic Warfare**. The Electronic Warfare (EW) field contains programmed elements to help counter enemy's EW threat: for example Electronic Counter Measures (ECM) to protect friendly communications from exploitation by hostile activities.

ORGANISATION OF INTELLIGENCE IN A BATTALION

56. The knowledge of the roles of the intelligence in an Infantry Battalion is essential for all intelligence personnel. The Intelligence Section in a battalion is located at the battalion hq and headed by an Intelligence Officer (IO). Under the IO are the bn Int Sergeant, Cpl and other privates. There is however no standard establishment for the strength of the intelligence section. Intelligence in a unit is organised into the intelligence office and information room as well as maintains documents and collects information.

57. **Intelligence Office**. The intelligence office is cited near the command post during operations. It is usually divided into 2 parts:

a. **Outer Office**. This contains map display, model, telephone and map table

b. **Inner Office**. This contains spare maps, stores, containers, docus and serves as a resting place for the personnel. It is headed by the sergeant.

58. **The Information Room**. The information room is sited along route from the visitors' car park to bn hq. It should be provided with large scale maps and latest unit's intsum and should be big enough for:

a. Briefing visitors on current situation.
b. Briefing and debriefing Patrols.
c. Holding 'O' groups and conferences.

59. **Files and Documents**. Files should be pruned when out of date and papers bearing security classification should be destroyed by burning. The following docus should be maintained:

a. Log AFB 58.
b. Briefing and debriefing proforma for patrols.
c. Patrol reports.
d. Observation logs.
e. PW- Captured material proforma.
f. Telephone and R/T Logs.
g. Request proforma for close air support (AFB 2053).
h. Format for air photography demands.

60. **Collation of information**. All information collected should be evaluated and thereafter reflected on the ops map as follows:

a. En defences.
b. Topographical going.

c. Patrol activities.
d. Mortar and arty tasks in DF.
e. Wire and mine fields (Own and en)
f. Code names and nicknames.

61. **Duties of the IO**. The IO is responsible to the CO for training of his men both in war and peacetime. He deals with all intelligence matters and obtains up-to-date info about en activities and intentions and about own troops. He also serves as a personal staff officer of the CO and carries out the following duties:

a. Training.
b. Staff officer.
c. Liaise with other units.
d. Studies en forces and topography.
e. Briefs and debriefs patrols.
f. Interrogates PW for immediate tactical info.
g. Carries out recce task for CO.
h. Writes bn sitrep.
i. Demands maps and air photos.
j. Understudies adjutant.
k. Ensures sit maps and int records are kept up-todate.
l. Briefs soldiers on evasion methods if they are captured.
m. Prepares sketches, enlargements and models.
n. Lectures other units on ORBAT of en.
o. Brief visitors to bn hq.
p. Assist unit security officer to enforce security.
q. Organise training of officers and men on air photo reading and its uses.

62. **Roles of the IO in War**:

a. **Advance**. IO moves with the CO, org 'O' group, establish comd post if there is a halt and holds brief for the adjutant.

b. **Attack**. Provides info on:

(1) Enemy strength and location.
(2) The goings.
(3) Timings of last light moon rise and first light.
(4) Patrol reports helpful for (a) – (c).
(5) Obtain info from captured or dead en.
(6) Mark routes in assy area to FUP and SL.
(7) Marshall covering guides in assy area and allocates task to them.
(8) Provides navigation party.
(9) Lays centre line.

c. **Defence**:

(1) Mans intelligence office.
(2) Establish Ops.
(3) Marks traces of bn position, DF tasks and nuclear contamination targets and minefields.
(4) Carry out recce for future advance or withdrawal.

d. **Withdrawal**.

(1) A representative accompanies advance party, prepares sketch map of new loc showing areas of coys etc
(2) Intelligence representative acts as a guide to IO and other rear party.

e. **Relief in Line**. The IO provides the following:

(1) Obtains info on locations of troops to be relieved.
(2) Patrol charts and reports.
(3) Wire and minefield charts.
(4) OP Charts.
(5) DF fire plan.
(6) Intelligence log.
(7) Details regarding track discipline.
(8) Info on en routine habits etc.

PRISONER OF WAR MANAGEMENT

63. In PW management, NAIC officers should be very familiar with the procedure of PW handling from point of capture till exchange of PW after hostilities. Officers should however be thoroughly knowledgeable about the role of the NAIC from the arrival of PW at the divisional cage. Special attention is to be paid to rules, handling, evacuation and documentation.

64. **Rules.** The rules of PW handling are as follows:

a. All PW are to be treated in accordance with the terms of Geneva Convention WO Code number 6637).
b. From the moment of capture they must be made to feel they are in the hands of a tough efficient unit which will treat them firmly and fairly.
c. Anyone PW who needs medical attention must be given at once.
d. There must be no fraternisation of any sort between prisoners and their captors or guards.
e. Prisoners should not be tied up or handcuffed unless this is unavoidable to prevent violence or escape.
f. Prisoners should be segregated as soon as possible.

g. Prisoners must not be allowed to talk amongst themselves or to smoke.

h. Prisoners should be separated from any aid to escape and from documents and equipment of intelligence value.

i. Belongings should be clearly marked and identified with its owner and sent back with him as they provide an interrogator with useful talking points and indication of character and employment.

j. Prisoners must always be kept under general observation to ensure the correct selection of PW for interrogation.

k. Capturing units must always prepare a Capture Report to be sent back with each prisoner. (See Annex A)

l. Prisoners must be provided with adequate food and drink, under controlled conditions and the time and quantity should be noted in the capture report.

65. **Handling**. When enemy prisoners are taken, the procedure to be followed is as enumerated below.

a. **Disarming**. Prisoner must be fully disarmed and must not be allowed to destroy any part of their equipment.

b. **Searching**. Prisoners must be thoroughly searched, papers, documents and maps secured and sent back with the prisoner's escort. It is forbidden to remove prisoners' identity badges of rank or decorations. Personal valuables will be taken away at Battalion Headquarters under supervision of the Intelligence Officer. Money and valuables taken from prisoners must be on the orders of an officer and must be recorded and a receipt given to the prisoners.

c. **Segregation**. Prisoners must be separated based on rank for conventional militaries or organisational groupings for insurgents. Talking must be forbidden and prisoners must

never be left unguarded.

66. **Evacuation**. The evacuation of PW may cause serious drain on manpower. If possible, our walking wounded should be used as escorts. The strength of the escort will vary according to the state of the prisoners' moral, the type of country and operational situation. Prisoners are to be collected at company headquarters which may detail a section to escort as many as 30 or more at a time to battalion headquarters. The escorts should take with them the following:

a. All maps and papers which have been taken from the prisoners.

b. A report on when, where and how the prisoners were captured.

c. Money and valuables taken from the prisoners duly labelled.

67. **Documentation**. The initial documentation and labelling of PWs, documents and materials are done by the capturing unit. The various forms used in this regards are as follows:

a. **Prisoner of War form**. This gives the personal details of the PW, the place and circumstances of capture as well as any information obtained through them. Three copies are prepared, 2 for receiving headquarters and one as office copy.

b. **Receipts for Valuables**. These are prepared when valuables and personal equipment are collected from PWs to ensure that they are not deprived of their valuables by unauthorised persons. It is prepared in quintuplicate. Two copies would be sent to the receiving headquarters, one copy placed on the cover containing the valuables and one for office use. The receiving headquarters will sign one copy in lieu of receipt and send it back to the originator. One copy will be given to the prisoner.

c. **Labels**. This include Prisoner of War and Captured Material labels.

d. **Prisoner of war State**.

e. **Captured Material State**.

INTERROGATION

68. Interrogation is a highly specialised activity carried out mostly by trained personnel. It includes the skilful questioning of witnesses and suspects. The effectiveness of investigation depends on the logic, craft and psychological insight with which the interrogator questions a person who is in possession of the information needed. The interrogator therefore needs to be briefed by an intelligence staff. Interrogation may be carried out in war or CRW and could be for agents, security suspects or deserters

69. **Briefing of Interrogators**. It is essential that the intelligence staff ensure that each interrogator knows exactly what information is required. Therefore he should be told preferably in the form of a simple question. Eg where is 84 Tk Bde and what is its role. Unless he is given proper direction, the interrogator will be wasting his time. In addition, the intelligence staff must ensure that all interrogators are fully and frequently briefed about enemy and the local operational situation.

70. **Interrogation in War**. When practicable, this is carried out in 4 phases:

a. **Tactical Questioning**. Selection for primary interrogation is made at this level.

b. **Primary Interrogation**. This is the responsibility of organised in small teams working in forward areas. The objectives of this interrogation is to extract the information

interrogators have been tasked to obtain. For the majority of prisoners it will be their only interrogation. Selection for secondary interrogation is made at this time.

c. **Secondary Interrogation**. This seeks longerterm intelligence, thus it is carried out by a secondary Joint Service interrogation unit at division, corps or theatre level. Some prisoners may at this stage be selected for detailed interrogation.

d. **Detailed Interrogation**. The only prisoners involved in this are those who have particular scientific, economic, technical or strategic information of value. They are interrogated at a Joint Service detailed interrogation centre either at theatre headquarters or in Nigeria.

71. **Interrogation in Counter Revolutionary Operations**. The people interrogated will seldom be soldiers and they may be anything to members of some students, political organizations, to well-trained 'hard core' terrorists. Normally they will be under Police control and will be interrogated by the Police, although a service element will be available to advice support, or supervise Questioning is usually divided into 3 phases

a. **Tactical Questioning**. This is undertaken by the capturing or arresting unit to establish the correct identity of the prisoner and to obtain information of vital importance, which may often by volunteered by the prisoner whilst suffering from the shock of being captured. Instructions will always be issued on such matters as the period for which a man may be held by military units before being handed over to the police. This is limited by the laws of the land.

b. **Initial Questioning**. This is conducted by the uniformed branch of the police or special branch.

c. **Interrogation at a Special Branch Centre**. This is the main interrogation for those selected for further

examination. It should be stressed that, apart from tactical questioning interrogation in counter Revolutionary Operations, it is essentially a matter for the civil authorities. Any military involvement will require the authority of the Ministry of Defence.

72. **Interrogation of Agent Security Suspects and Deserters**. The Interrogation of agents, security suspects and deserters is normally carried out by one of the primary interrogation teams in the forward areas. Those who have information of importance will be sent to back for secondary and perhaps detailer interrogation.

INTELLIGENCE ASPECTS OF PATROLS

73. Patrol is of vital importance to the intelligence staff since they are normally tasked to collect information. Reconnaissance patrols acquire information by stealth while fighting patrols acquire it by force where necessary. When conditions favour their use, patrol can be the IOs most productive source of information. However, much depends on how intelligently they are tasked and how professionally they are briefed and debriefed by the intelligence staff.

74. **The Roles of the Intelligence Staff**. As part of collection planning, the IO will task patrols to gather information. The IO will therefore be responsible for:

a. Identifying patrol tasks.

b. Preparing a patrol plan in conjunction with the Ops officer.

c. Giving the patrol commander the intelligence briefing. (See Annex B for IOs briefings of patrol commander)

d. Debriefing the patrol or patrol commander on return.

75. **Patrol Planning**. Patrols will be ordered by higher formation, the CO, sub-unit commanders or the IO (through the CO). Those ordered by the former will usually have security or offensive tasks, while the IO will require patrols to gather information. All patrols are coordinated by using a Patrol Programme. This will be the task of the IO or unit ops officer. Similar coordination will be carried out at divisional headquarters. The programme should be issued to sub-units early enough to allow patrols to be briefed and prepared as necessary. Such planning is most important to prevent friendly patrol clashes

76. **Factors Involved in Patrolling**. Patrolling is a hazardous and seldom popular operation, especially in general war. Patrols should only be ordered:

a. When information, security or effective domination can be usefully gained.

b. When there is enough time available. The mounting of a patrol takes hours, not minutes for most tasks. This will often rule them out as a collection agency, especially in fast moving general war situations.

77. **Intelligence Patrol Briefing in IS and CRW Ops**. As part of the briefing in IS and CRW situation, the intelligence briefing will be in 2 parts.

a. **Part 1- Information to the Patrol**. This will include:

(1) Known sniping locations/killing areas.

(2) Recent known 'aggro' spots' incident map.

(3) Mining and IED danger spots.

(4) Known areas of insurgent activities, including type of activity/strengths/timings/purpose.

(5) Known terrorists in the area, with photographs and descriptions.
(6) Safe houses.
(7) The 'going' (applies mainly to rural areas).

b. **Part 2- Information Required from the Patrol**. This will include:
(1) Terrorist to detain on sight- with photographs, descriptions and background.
(2) Terrorists or person to observe and report with photographs, descriptions and background.
(3) Cars to check/detain/observe/report.
(4) Houses to check/observe/report.
(5) Any specific activity or area to watch.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

78. Intelligence Preparation of the Battlefield (IPB) is a systematic and continuous process of analysing environment in a specific geographic area and threat, which is designed to support military decision making. IPB identifies the facts and assumptions about the battlefield and threat that allow effective staff planning. IPB offers the most graphic presentation of the battlefield to the commander. Candidates should be very familiar with this concept and be able to differentiate it from the intelligence estimate. Knowledge of the different overlays prepared in the IPB process will also be important.

79. **Purpose of IPB**. IPB process helps the commander to selectively apply and maximise his combat power at critical points in time and space on the battlefield by:
a. Determining the threats likely course of action.

b. Describing the environment the forces are operating with and the effects of the environment on them.

80. **Steps in IPB**. There are 4 mandatory steps to be performed each time the IPB is conducted:

a. **Step 1- Define the Battlefield Environment**. This involves:

(1) List significant characteristics of the environment.
(2) Identify the area of operation.
(3) Identify areas of interest.
(4) Identify the degree of detail feasible for IPB.
(5) Identify intelligence gaps.
(6) Collect the required intelligence.

b. **Step 2- Describe the Battlefield Effect**. This involves:

(1) Analyse the battlefield environment eg terrain, weather etc.
(2) Analyse military aspects of the environment eg OCOKA etc.
(3) Evaluate the effects on military operations.

c. **Step 3- Evaluate the Threat**. Specific works include:

(1) Convert threat doctrine or pattern to graphics and describe preferred tactics or options.
(2) Update or create ORBAT files to cover organisation, composition, strength, disposition, tactics, training logistics and effectiveness. Others are, morale, leadership personality etc. (3) Identify

threat capabilities or options which the threat can adopt to influence the accomplishment of friendly missions.

d. **Step 4- Determine the Threat's Courses of Action**. To do this:

(1) Identify the threat's likely objective and desired end state.

(2) Identify the full set of courses of action available to the threat.

(3) Evaluate and prioritise each course of action.

(4) Develop detailed course of action.

(5) Identify initial intelligence collection requirement.

81. **Effects of Terrain and Weather on Military Operations**. This can be achieved through the analysis of:

a. **Military Aspects of Terrain**. This will cover:

(1) Observation and field of fire.

(2) Concealment and cover.

(3) Obstacles.

(4) Key Terrain.

(5) Avenues of approach.

b. **Military Aspects of Weather**. This will cover:

(1) Visibility.

(2) Winds.

(3) Precipitation.

(4) Cloud cover.

(5) Temperature and humidity.

SECURITY INTELLIGENCE

82. In peacetime and especially during military regimes a lot of emphasis is placed on threat to national security. Candidates should however see this as a universal phenomenon and not just as a parochial assessment of the Nigerian situation. They should therefore also see themselves as intelligence officers serving any type of government – military or civilian. This section involves a lot of security planning at bde and div levels. Candidates who have worked in NAIC units should have no difficulties as these functions are carried out almost daily. It is however to be pointed out that procedures being practiced in unit would only be acceptable if they conform with those taught at NAIS and issue from HQ NAIC.

SECURITY

83. As an intelligence officer, security is thought of in terms of national security in a broad sense and the security of the military unit and organisation as a whole. Military security is organised primarily on unit bases, the commander ultimately responsible for the security of his unit. In every unit, an officer should be appointed as Unit Security Officer. In a bn, the Bn 2ic is primarily the security officer. He may however be assisted by a junior officer preferably an IO or an officer trained in unit security duties.

84. **National Security**. Presupposes that condition which ensures the safety of our national infrastructure which ensures that subversion does not exist, that espionage does not and cannot take place and that sabotage is entirely prevented. Security when considered in this form includes the national economy, politics, industrial infrastructure and defence. Military security on the other hand cannot be entirely divorced from the overall national security.

85. **Nature of Threats to Security**. Here are 2 major aspects to the threats to security:

a. **Direct Threat (War time)**. This emanates from a hostile power at war with another. This can be carried out as follows:

(1) Interrogation of PW with the intention of obtaining ORBAT information.

(2) Destruction of vital materials in order to prevent a commander from fielding his full force. (c) Subversion or influencing members of the armed forces through psychological operations designed to destroy his fighting capabilities and moral and even undermine his loyalty.

b. **Indirect Threat (Peacetime)**. This refers to all activities designed by nations in peacetime to improve their own economy as well as undertake a systematic study of those forces that constitute threats to their stability, in both peace and war. This is done in the following ways:

(1) Strategic collection through covert and overt means

(2) The penetration of sabotage groups.

(3) Subversion through infiltration of legal organizations, recruitment of disloyal nationals and publication of slanted information to discredit government.

86. **Sources of Threats**. The threat to security emanates from 2 main sources:

a. **HIS**. This is the intelligence service of foreign powers, especially those which may be described as hostile and whose activities would most certainly include

(1) Exploitation of situations that would further the interest of the HIS

(2) Recruitment of personnel by whatever means available to the HIS. This means may include persuasion or even appeal to the sentimentalities of the personnel to be recruited.

(3) Examples of HIS include:

(a) **Communist Countries**: **and Socialist.**

(i) KGB - Police. Soviet Military.

(ii) GRV - Intelligence. Soviet Military.

(iii) CIS - Chiness Intelligence Service.

(iv) East Gern Intelligence.

(b) **Western countries**:

(i) CIA - USA.

(ii) MI5 - Intelligence Service British.

(iii) MI6 - Military Intelligence UK.

(iv) FIS - French Intelligence Service.

(v) MOSSAD - Intelligence Service Israel.

(vi) DOSS - DSS South Africa.

b. **Domestic Subversive Organisation**. Domestic Subversive Organisations (DSO) are those which aims to usurp power or overthrow the legal government by illegal means. Such subversive organisations may not be infiltrated by the HIS but their activities are sure to be so exploited.

87. **Principles of Security**. The success of any good security depend on the following principles/factors:

a. **Security Design Must Make Sense**. Your security design within the establishment must be commensurate with your need so as to ensure the desired results. Eg it is foolish to provide 2 security guards at a Central Bank's gate.

b. **Define the Target**. Before any security measures are introduces in a protected area, things to be protected must be known. The knowledge of what are to be protected provides for the degree of protection needed. You know the roles and importance of the item to be protected.

c. **Assess the Threat**. Usually, the degree of threat varies from place to place. Access what kind of threat is expected including possibility of subversion, leakage of information and quality of building housing the valuable item.

d. **Defence in Depth**. Obstacles must be arranged around what is being protected. They must be interlocked and operating outwards from the target.

e. **Education of All Staff**. Staff /Workers of all grades in an establishment must be educated to appropriate threats, because it is by so doing that they may not unconsciously fall prey to subversive information.

SURVEILLANCE/COUNTER SURVEILLANCE

88. Surveillance is a form of investigation which consists keeping persons, premises or vehicles under physical or technical observation for the purpose of acquiring detailed information concerning activities, operations, identities and contact of subject in order to obtain evidence or information pertinent to an investigation

89. **Organisation of Surveillance Headquarters**.
Surveillance headquarters should be organized as follows:

a. Selected to ensure movement of staff does not attract undue notice.

b. Should be operated under cover of suitable business.

c. The accommodation should be sufficient for an ops room to be equipped with more than one telephone, radio facilities, large scale map of the local area and reference books as required.

d. There should be a changing room, rest room, kitchen and sleeping facilities, storage room to contain surveillance hardware.

e. A change of clothes or albums or photographs of suspects be provided for the use of the staff.

f. For mobile surveillance, a team will be chosen composed according to the likely area of operation and a team leader selected.

90. **Briefing of Surveillance Teams**. Information to a surveillance team during briefing include:

a. Description of suspect.

b. Residence or pick up area.

c. Known contacts and hunts.

d. Whether or not he is a trained agent.

e. Means of travelling; method of movement – foot, bus, taxi etc.

91. **Inspection of Surveillance Team by Team Leader**. As a team leader, the following things should be looked out for:

a. Wearing inconspicuous clothing ie their mode of dressing must be based on the area concerned.

b. Carrying hats, raincoats if appropriate.

c. Carrying money, notebooks, pencil and watch.

d. Aware of the signal that should be used in any given situation.

e. Rehearsals of the signal to be repeated.

92. **Counter Surveillance**. This involves the range of actions taken by a suspect who has become conscious that he is under observation. In such circumstances, the suspect will first try to confirm his suspicions by the following:

a. He will double back on his track after entering a building or turning in a corner.

b. He will stop suddenly to tie-up his shoelaces or pick up something he had dropped.

c. He will repeatedly cross the road looking right and left before he does so.

d. He will use shop windows as mirrors.

e. He will enter lifts, turn round abruptly and see who gets in.

f. He will make use of unfrequented places, where the teams will be conspicuous.

g. He will also try to lose his watchers by:

(1) Diving into a dense crowd.

(2) Entering a building and leaving by another exit.

(3) Jump on a bus/taxi suddenly.

93. The common espionage slang, 'The suspect is spitting blood' and 'The suspect has come to rest' is used during surveillance when the suspect is believed to be taking evasive actions and when he has successfully avoided the team respectively. It is also essential that every moment of a suspect be recorded.

SECURITY OF DOCUMENT AND MATERIALS

94. **Basic Rules of Document Security**. The basic rules of document security are:

a. Classify correctly.
b. Keep classified paper to a minimum.
c. Ensure that papers are easily traceable.
d. Ensure that checks will reveal looses.
e. Prevent unauthorized access.
f. Ensure that the staff know the rules.

95. **Principles of Document Security**. The principles of document security is based on the 3 needs as follows:

a. **Need to Know**. No person should be given information than necessary to enable him carry out his or her duties effectively.

b. **Need to Hold**. Althoughs a person may have the need to know the contents of a particular classified document. It does not necessarily follow that he or she has need to hold (retain) the document. Individuals should therefore be permitted to retain only that classified information which is essential for the performance of their duties.

c. **Need to Take**. A person who has the need to know and the need to hold can only in circumstance where there is a real need remove document from the office.

95. **Ten Commandments of Document Security**. Document security is based on the following 10 commandments:

a. Each document is to be accorded a security

classification based on the estimated damage that would be caused to the nation by the unauthorized disclosure of the information in the document.

b. Each document is to be classified correctly to reflect its security value and indicate the appropriate standard of protection it is to be given.

c. Classified documents are not to be accessible to unauthorized persons at any time based on the need to know, hold and take principles.

d. The holder of a classified document is to record and control the document in such a way that the location of the document is known at all time.

e. Documents are to be transmitted by secure means appropriate to their classification.

f. Classified documents are always to be stored under secure arrangement.

g. Documents are to be downgraded or declassified when the content becomes less important.

h. Documents that are no longer required are to be destroyed by an appropriate method and under secure arrangement appropriate to their classification.

i. Classified documents are to be checked regularly and on snap basis.

j. An investigation must be conducted if a classified document cannot be found or compromise is thought to have occurred.

96. **Copying and Reproduction**. While documents may be adequately protected, improper production or photocopying could pose serious threat. Photocopying should be controlled and supervised. The equipment should be controlled by properly vetted personnel.

97. **Security of Materials**. This involves the protection of materials including equipment, vehicles, supplies and buildings from attack, principally through sabotage.

a. **Forms of Attack**. There are 2 forms of attack on material:

(1) Through espionage which seeks information about the material, particularly the location and other security weakness.

(2) Through sabotage which seeks to destroy, damage or remove material.

b. **Defence of Material**. As accurate an assessment as possible must be made of the prevalent threat and the targets at which it may be directed. The following are important in the defense of material:

(1) Which are the Key Points (Kps), the obstruction of which would most affect operations, at a given time and place.

(2) Which are the vulnerable Points (VPs) that is those points within the key points which are vital to their operations.

(3) The defence must be organized in depth, working outwards from the VP.

(4) The defence must never be relaxed. A momentary relaxation could let the saboteur in.

(5) Defence should be a combination of security orders, physical security measures and vetting procedures.

98. **Responsibility for the Protection of Material**.

Arrangement for the protection of material is the responsibility of all persons charged to do so, whether temporarily or permanently. These responsibilities are as follows:

a. The overall responsibility of the Counter

Intelligence staff is to assess the threat generally.

b. The ultimate responsibility is that of the commander.

c. The responsibility of the Security Officer(SO) is to draw up the Unit Security Standing Orders(USSO) and device adequate physical security measures.

d. The responsibility of an individual is to know the prescribed safeguards and apply them.

e. The responsibility of security personnel is to advice on the security measures and draw attention to security weakness.

SECURITY OF PERSONNEL AND OFFICES

99. **Personnel Security**. This is a collective term used to describe the various measures and procedures which together attempt to:

a. Exclude undesirables from enlisting into the organization.

b. Exclude or remove from posts vital to the security of the state, those personnel whose reliability or trustworthiness is open to doubt.

c. Forewarn all personnel against HIS and subversive influence wishing to cause disloyalty, breed disaffection or undermine morale.

100. **Measures to Ensure Personnel Security**. The following areas require attention for the security of personnel:

a. **Recruitment**. The recruitment of personnel demands that required standards and criteria such as educational qualification and character attributes are scrutinized prior to employment. This is aimed at ensuring that undesirable elements are not recruited into the services. This measure also, to a certain extent, ensure the exclusion

of persons who are, or who might become undesirable from the security point of view.

b. **Vetting**. The aim of any vetting system is to deny employees and potential employees access to classified information and material when their trust or reliability is open to doubt. In its simplest form, the vetting process is a reference to national records and is made in order to identify individuals with criminal records or disloyal persons. Vetting will undoubtedly weed out certain individuals who are, or who become risks to security but it will not in any sense be 100 percent effective. The following limitations should be born in mind.

(1) The effectiveness of record checks will depend on the depth, accuracy and availability or appropriate records and also on the positive identification of the subject.

(2) Vetting is only valid on the day it is completed. While advanced vetting clearance must be supported by ample evidence of a favorable nature, it is not guaranteed that all evidence to the detriment of the individual has come to light.

c. **Vetting After Care**. This is a procedure designed to maintain the value of the vetting system by noting and reporting any changes in the character or circumstances of the individual. The organization would therefore ensure that:

(1) Appropriate reports are made of changes of circumstances, character weakness or indeed, any other information which may have bearing on an individual's security reliability.

(2) Valid proofs of clearance are held for each individual occupying a post where vetting is required and that appropriate vetting registers are

maintained.

(3) Personnel occupying advance vetting posts are properly and regularly briefed on their responsibility.

(4) A yearly review is made of the posts required for vetting within the organization.

d. **Security Education**. All personnel, whether charged with specific security function or not, must be given security education in order that they become aware of the following:

(1) The security threats posed by HIS and subversive organizations to personnel.

(2) The meaning and purpose of our own counter measures.

(3) Their own responsibility for security including the need to diligently comply with published orders and instructions.

(4) The need to report any matter which may have security significance.

e. **Management**. This involves activities that discourage subversive influence by fostering conditions which promote discipline and high moral. Officers responsible for supervision of personnel should be particularly vigilant to detect and put right those cases which if ignored could have negative security implications. Example might be.

(1) An individual who is dissatisfied with his posting, pay, promotion, disgruntled as a result of some other real or imagined grievances.

(2) The staff that recently returned from overseas and is struggling to maintain a standard of living, which he cannot now afford.

(3) The individual who has minor dept.

(4) The staff that drinks heavily but not yet excessively.

(5) Superior officers should be able to distinguish between minor indulgences and excesses which carry serious security implications.

101. **Espionage in Offices**. Espionage can be conducted in offices through the following ways: a. Authorized access. b. Third party with access. c. Surreptitious means. d. Negligence. e. Technical dropping.

102. **Protection and Control of Access**. This is achieved as follows

a. Centralizing all classified documents in one place, thus preventing those not permitted to enter such a place from gaining access to the information.

b. Files passed to various offices should be locked away once the users are leaving the office temporarily.

c. Locations/offices to be used for discussing classified matters should be technically swept and secured 12 hours prior to the conference.

103. **Precautions Against Technical Eaves- Dropping**. The following precautions would eliminate or reduce the ability of HIS to eavesdrop in an office through the use of bugs:

a. Access control-detection devices could be deployed at the gates to prevent unauthorized persons bringing in recording equipment.

b. All keys should be treated as security keys.

c. Cleaning, decoration and maintenance of offices should be supervised.

d. Record of works done should be kept.

e. Record of workers names should be kept.

f. Inspect equipment and furniture prior to removal (for repairs) and on return to the room.

g. Visitors without permission are to be escorted.

104. **Key Control**. The following precautions are necessary to enhance good key control:

a. Minimum number of keys should be in use.
b. Protect such keys from unauthorized persons.
c. Centralized and secure all duplicate or triplicate keys.
d. Issue keys on signature.
e. Use security key register.
f. No key should be removed from the unit unless it is absolutely necessary.
g. Keys should be changed every 6 months.

SECURITY INVESTIGATION AND INTERVIEW

105. **Principles of Investigation**. The following principles guide the conduct of investigations:

a. **Factual Truth**. It must be based on set of known and demonstrable facts not suspicions, speculation or opinion.
b. **Accurate Interpretation**. This entails the study of a fact against the background from which it emerged to reveal the presence of the abnormal or the absence of the normal.
c. **Sound Logic**. A well developed reasoning faculty is necessary to enable the investigator to establish the true relationship of facts to each other and their significance to the course of the enquiry.
d. **Deductive Reasoning**. This is the process whereby a conclusion is inferred from facts that is already established. For example, if a missing document was checked a week before it was found to be missing, the inference by simple deductive process is that it was lost at some time during that week.

106. **Quality of an Investigator**. An investigator should possess the following qualities:

a. He should be very zealous and indefatigable.
b. He must be persevering.
c. He must be swift in reading minds of men.
d. He must have agreeable manners.

107. **Interview**. Any dialogue between 2 people may be considered an interview, in the sense that information is sought by one and given by the other. The main difference between an interview and an interrogation is that, in the former, the subject may leave at will. In interrogation, he has been or soon will be deprived of his liberty. As a result of this distinction, different techniques are required.

108. **Types of Interview**. Interview fall into the following 2 categories:

a. Where the security/CI organization is approached with information.
b. Where the organization requires the information and approaches the subject. The subject may or may not co-operate.

109. **Interview Preparation and Planning**. The following points should be considered when preparing for an interview:

a. The aim of the interview.
b. The subject – is he/she available.
c. Background knowledge of subject – available records, all relevant information on subject/association.
d. How many interviews are there to be carried out?
e. How is the interview to be recorded? (notes, tapes etc)

f. Location of interview, setting up, stage management.
g. Other agencies involved.

110. **Stages of Interview**. Interview fall into 3 stages as follows:
a. **Preliminary**. This involves:
(1) Identify the subject.
(2) Introduce yourself.
(3) State the reason for the interview.
b. **Body of the Interview**. This involves:
(1) Allow subject to tell his story.
(2) Expand subjects account by questioning in order to achieve the aim.
c. **End of the Interview**. This involves:
(1) Recapitulate on the information – correct inaccurate details.
(2) Warn subject not to disclose the information to unauthorized persons.
(3) Check future availability of subject.
(4) Say thank you – if in context.

111. **Dos and Don'ts in Interview**. Interview processes involve some dos and don'ts:
a. **Dos**:
(1) Use simple, precise questions.
(2) Obtain all details.
(3) Control the interview.
b. **Don'ts:**
(1) Do not lose your temper.
(2) Do not allow the subject to control the interview.
(3) Do not argue.
(4) Do not allow yourself to be questioned.

(5) Do not divulge the extent of your knowledge.

SECURITY SURVEYS INSPECTION AND CHECKS

112. Most protective security measures are routine and essentially a matter of discipline and training. Establishment must therefore plan and review their own security measures. The system for carrying out security surveys, inspection and checks will vary slightly from one establishment.

113. **Security Survey**. This is a detailed examination of the security procedures in an organization or headquarters carried out by the security section. The aim is to advice the management where a weakness exists and to recommend the necessary protective security measures that are requires.
Security survey will normally follow the following pattern.

a. **Preliminary**. This will include:

(1) A study of the role of the organization, its importance as a target of hostile intelligence service etc.

(2) Obtaining details, as far as is practicable, of classified documents and equipments held by the organization.

(3) A report on the security problems and protective security measures available.

(4) Planning the survey.

b. **Survey**. When carrying out the survey, the security section will do the following:

(1) Report to the local security officer and discuss with him the proposed plan of the survey.

(2) Carry out the survey, using an aidememoire or established procedures.

(3) Discuss the result of the survey with the local security officer, and if necessary, with representatives of the management team.

c. **Report**. This will be written by the security officer who carried out the survey immediately it is completed.

d. **Disposal of the Report**. The report is to be signed by the security officer that carried out the survey. Two copies are normally sent to the headquarters of the organization. The management will be responsible for taking such action as is needed to ensure that satisfactory protective security measure are introduced as recommended in the report.

114. **Security Inspection**. This is a periodic inspection of the security arrangement in an organization or headquarters, carried out by the security section. Its purpose is to assess the effectiveness of the protective security measures adopted by the organization or headquarters concerned. Normally it is carried out once a year. However, if circumstances demand, headquarters may instruct the security section to carry out a selective inspection of the security arrangement of the security arrangement of all facilities in its area of operation.

115. **Security Checks**. This is a review of the protective security measures of an organization or headquarters, carried out by the security officer. Its purpose is to ensure that orders and instructions are adequate and that they are being complied with. During the year following the security survey, the organization is expected to use the survey report as the basis for conducting the checks. Checks would be conducted at least once a quarter or if security breach has recently occurred within an organization or if it is temporarily taking part on special activity.

ACCESS CONTROL AND CONFERENCE SECURITY

116. **Control of Access**. Control of access refers to all security measures adopted within restricted (controlled) areas, aimed at denying access at random to unwanted persons who may be desiring to gain access to valuable materials, equipments and documents as well as personnel.

a. **Threats**. The following are the prevalent threats to security:

(1) Espionage which may be directed at knowing the security set-up and guard routine of the target installation will take place.

(2) Sabotage which tends to destroy, damage or remove the item under protection.

b. **Principles/Measures to be Adopted**:

(1) The installation should be fenced with limited inlets.

(2) The security control post should be located at the main entrance where all movements of workers, visitors, vehicles etc would be checked.

(3) The security officer's office should be located at a vantage place where he would have complete control of his men at different duty bits as well as general movement of people and vehicles.

(4) The gates should be properly manned by security personnel.

(5) Security light must be provided at close intervals of the perimeter fence.

(6) Guard dogs should be provided to aid the physical ability of human guards.

c. **Security Against Violence of Individuals**. This involves the following:

(1) Physical fitness.

(2) Mental alertness.
(3) Ability to assess prevailing situation.
(4) Use of discretion.
(5) Provision of necessary equipment.
(6) Proper screening of individuals prior to employment.

d. **Use of Passes and Permits**. A pass is a document which authorizes a holder to have access to a restricted area and thereby helps to control entry to a specific area or restricted part of the area. It is not an identity card. A permit is a document which authorizes the holder to have access and carry out functions in a restricted area. The period of the function is often specified. While a pass authorizes entry to a place, a permit allows the holder both access and function for a given period.

e. **Types of Passes and Permits**:
(1) Temporary pass eg leave pass.
(2) Permanent pass eg security pass, ID card.
(3) Gate pass eg hotel, cantonment.
(4) Visitor pass eg RP issuance to visitors.
(5) Electronic pass.

f. **Design of Pass Forms**. The following should be borne in mind in designing pass form:
(1) Easily recognizable with little written details as possible.
(2) Incorporate features which can reveal forgery on close scrutiny.
(3) Must not disclose the area or part for which it is valid, except by a code index.

(4) A recent photograph of the holder is required.

117. **Conference Security**. All classified conferences need to be controlled to curtail unauthorized access. The HIS eyes classified conferences in order to obtain information to which they are not entitled. The extent to which security measures are applied will depend on the classification of the event. Minimum measures should ensure that:

a. **Action Before the Conference**.

(1) Appointment of an officer to coordinate security arrangements and write security orders.

(2) Appropriate vetting of all persons taking part including technical, cleaning and maintenance staff who may have access to the secured area.

(3) Designation of appropriate security classification for administrative planning instructions in order to minimize the possibility of alerting hostile intelligence services.

(4) Bringing the place or area under security cordon 48 hours or more before the event depending on assessed threats from hostile interest.

(5) Inspecting the area after the cordon has been established to ensure no listening device has been installed and that speech cannot be heard or event overlooked.

(6) Ensure placement of metal and bomb detection mechanisms at the entrance points if not already installed.

b. **Action During the Conference**.

(1) No unauthorized person should have access to the vicinity of the event or the building.

(2) Maintain strict control at the entrance, etc, and

vehicles brought into the secured area.

(3) Establish control point for visitors and the press outside the secure area.

(4) A visitor or member of the press can only be admitted into the secure area on the authority of a responsible official and only under escort.

c. **Action After the Conference**.

(1) No classified information leaves the building or the vicinity of the event.

(2) No unauthorized person has access to classified information connected with the event.

(3) Search for classified waste, used drafts classified as top secret, memory cards, discs etc.

(4) Arrange for the storage and destruction of classified waste.

TECHNICAL INTELLIGENCE

INTRUDER ALARM SYSTEM

118. An intruder alarm system is a device designed to detect and signal that an intruder or an unauthorized person has entered or attempted entering a protected area.

119. **Component of the System**. All alarm systems consists of 3 sections:

a. Detector device.

b. Control equipment.

c. Signaling apparatus or alarms indicating equipment.

120. **Detect or Device**. The detector device detect movement and cause a signal to the equipment. They are follows:

a. Mechanical contact.

b. Magnetic contact.
c. Vibration detector.
d. Pressure tube.
e. Lead foil.
f. Bill sensors.
g. Panick button.
h. Dead man alarm.
i. Space protector.
j. Trip wire.
k. Close wiring.
l. Light Beams.
m. Proximity detector.

121. **Control Equipment**. The control equipment must be able to perform the following functions:

a. must be able to accept the signal from the detector.
b. Must relay the signal to the alarm indicating equipment.
c. Switch for On and Off or Day and Night use.
d. Test prior to switching on.
e. Power supply for the circuit.
f. Monitor the cabling.

122. **Signal Apparatus**. The signal apparatus are of the following types:

a. Local bell or light.
b. Automatic dialing and transmission of a pre-recorded message over a telephone line
c. Silent signaling of video recording system.
d. Automatic activation of a video recording system.

123. **Design of Alarm System**. There are 3 basic methods of designing an intruder alarm system:

a. **Trap Protection**. This permits the entry of an intruder but depend upon detecting him as he moves about the area.

b. **Perimeter Protector**. All possible means of entry on the perimeter fence are protected to give early warning of an intrusion or intruder.

c. **Volumentry Protection**. This utilizes space protector to give protection to a room or space. It can selectively be used to protect important items while the insignificant once are left unguarded.

LOCKS

124. A lock is a mechanism by which a door may be fastened with a bolt that needs a key to work it. They could also be referred to as 'time buyers' they help in delaying an intruder from getting access to a protected containers or room. When a door is forced open after being secured with a lock, it is said to be an overt act, when it is picked secretly, it is referred to as surreptitious act.

125. **Requirement for Security Lock**. The basic requirements for a security lock which must withstand picking and some degree of force are as follows:

a. It should have a minimum of 6 levers or detainers.

b. It should incorporate at least 2 recogniser antipicking devices.

c. The bolt should be saw resistant.

d. The bolt should be a dead bolt (ie not spring loaded) and the throw should not be less than 1.6cm.

e. The lock should be mortised into the door whenever possible.

126. **Types of Locks**. There are 3 basic types of locks:

a. **Rim Locks**. Screwed to the inside face or surface of a door.

b. **Mortice Locks**. Secured inside the body of the door and should be supplemented by a box plate to receive the boil, mortised into the door jamb.

c. **Padlocks**. A detachable lock with a moveable or hinged shackle to go through a staple or ring and thus secure it.

127. **Types of Lock Mechanism**. The types of lock mechanism are:

a. Warded lock.
b. Cylinder lock.
c. Combination lock.
d. Electric lock.
e. Magnetic lock.
f. Interchangeable cord.
g. Cipher lock.

CLOSE CIRCUIT TELEVISION

128. Close Circuit Television (CCTV) is used to enhance security by providing the 3 key elements which are prevention, elimination of opportunities and detection in security application. CCTV serves a limited audience such as the security officer to monitor events from one or several remote locations. It can also observe protected or restricted area, high-value goods in warehouse, fence lines, parking lots and other corporate or industrial areas.

129. **Types of CCTV**. The CCTV comes in the following types:

a. Practical low light level TV system.
b. Night vision adaptation.

c. Electronic photo imaging version.

130. **Quality of Effective CCTV Applications**. The following essential aspects of CCTV are required to judge quality:

a. **Characteristics of CCTV**. Ability to operate under any marginal light conditions and provide adequate security surveillance of the low light level type.

b. **Component Parts**. Components to include Television camera, automatic zoom lens, manual control override and monitoring equipment.

c. **Camera Movement Capabilities**. Detecting pilferage, theft or intruder in direction of 360.

d. **Operational Capabilities**. Camera should have capacity for remote control, routine and continuous monitoring of specific activity as well as preplanned monitor and automatic zoom of activity at specified intervals.

e. **Central Security Monitoring and Control Room**. This enables fast response of security officers when needed.

f. **Camera Shot Classification**. Determining the essential video capability for each area of protection including extreme close-up, close-up, bust shot, medium close-up, mid shot, three-quarter length, long shot wide angle.

g. **Application of CCTV**. This is in terms of communication between monitoring security officer and the camera location, security of surveillance report and clarity of image to verify identity of persons seeking access.

131. **Weakness of CCTV Surveillance Application**. The following are the weakness of CCTV:

a. **Turning Lights Off**. Darkness normally disables the system and creates a diversion. This may be reduced if an infra-red device is incorporated

b. **Waiting Technique**. The determined intruder waits out of view until a camera sweeps by and he then slips by it undetected by the monitoring security officer.

c. **Creating a Diversion**. The most effective way an intruder can overcome CCTV systems is by creating a diversion. He or she creates a situation making the monitoring security officer to focus attention on a specific area.

CONCLUSION

132. This study guide is only to direct candidates on what is expected of them in the course of writing the SSCQE. It is by no means exhaustive but basically a reminder. Candidates who have studied the reference materials would find the paper relatively easy.

ANNEXES

A. Captured Report.
B. Headings for IOs Briefing of Patrol Commanders.
C. Collection Worksheet.

READING MATERIALS

4. Candidates are not restricted in their choice of reading material but the following are essential.

a. NAIS manual on Combat Intelligence (Rev 2011).
b. NAIS précis on Basic Security.

ANNEX A TO
MIL TECH

CAPTURED REPORT

(To be completed at the time of CAPTURE by the capturing unit and then retained by the escort until the prisoner is handed over)

1. Name of Prisoner_____
Rank_____

2. Official Service Number_____

3. Where Captured(Grid Ref)_____

4. Dates and Time of Capture_____

5. Direction(Compass Bearing)_____

6. Travelling Companions_____

7. Any other Point of Interest_____

Signed

Rank_____
Name_____
Unit_____

ANNEX B TO
MIL TECH

HEADINGS FOR IOS BRIEFING OF PATROL COMMANDERS

1. The Io should cover the following intelligence aspects when briefing a patrol commander

a. Topographical information, particularly about the going, cover available and best routes which would have been build up from previous patrol reports.

b. Enemy forces including their wire, minefields, fixed lines etc.

c. Own forces including location of forward troops, minefields, lanes, gaps in wire and details of any other patrols operating and fire support.

d. Mission in the form of questions if not given in the ops part of the briefing.

e. Timings such as time out and when to leave own areas, time in and place of entry.

f. Routes and limitations affecting choice of route, particularly regarding our own DF areas.

g. Meteorological details such as weather forecast, where possible, timings of moonrise, sunrise and sunset.

h. Password and light signals of wireless instructions.

i. Security and reminders on the dangers of carrying documents/marked maps, etc.

2. The briefer must use all possible aids eg air photos, map enlargements, models etc.

AN ANNEX C TO MIL TECH

INTELLIGENCE COLLECTION WORKSHEET

PRIORITY INTELLIGENCE REQUIREMENT (PIR)AND INFORMATION RREQUIREMENT(IR)	INDICATORS	SPECIFIC INFORMATION REQUIRED	COLLECTION AGENCIES				PLACE AND TIME TO REPORT	REMARKS
			OSINT	HUMINT	IMINT	COMMINT		
List PIR and IR	List indicators that will satisfy each PIR	If necessary list specific information required to satisfy the indicator	Place an x under any agency that can collect the required information and circle the x if an agency has been selected and tasked				Place may be a headquarter or unit, Time maybe specific, periodic or as obtained	Include means of reporting. Include established comms

ROLES OF MILITARY POLICE IN PEACE AND WAR TIMES

1. The Military Police (MP) is primarily responsible for the protection of military personnel, safeguarding military property and assisting in maintaining discipline through the enforcement of laws, orders and regulations. The MP perform various roles both in peace and war time. Thus, commanders at various levels require the input or professional expertise of a provost commander to achieve their end state.

CONDUCT OF PROVOST OFFICERS

2. Section 291 of the AFA, CAP A20, LFN 2004 defines a Provost Officer as "a Provost Marshal or an officer appointed to exercise the functions conferred by or under service law on a provost officer". The effectiveness of a provost officer in carrying out his duty depends to a large extent on his conduct or adherence to code of ethics of his profession. Sgt O'Brien of the Royal Military Police summarized code of ethics of provost officer in one sentence. He said "When you put the red cap on, you become part of something that represents the highest standard. You must remain beyond reproach at all times and follow our motto "Exemplo Docemus" which means "By Example We Shall Lead".

PEACE TIME ROLES

3. The MP performs the following roles during peace time:
   a. Prevention and detection of crimes.
   b. Apprehension of criminals.
   c. Interrogation and investigation of suspects.

d. Protection of military personnel and safe guard of military property.
e. Enforcement of laws, orders and regulations including out of bounds regulations.
f. Traffic and crowd control duties.
g. Mobile and foot patrols.
h. Ceremonial duties including Protection of VIPs and escort duties.
i. Internal security.
j. Liaison with civil police and other Paramilitary Services.
k. Route signing and speed limits.
l. Serving as prosecuting officer in a Court Martial.

WARTIME ROLES

4. MP performs number of operations, which may be done independently or in conjunction with other arms to accomplish their missions. Because MP assets are limited, the specific operations MP units perform at a given time are determined by the manoeuvre Commander. Some of these tasks performed by the MP during war time are:

a. Battlefield Circulation Control (BCC).
b. Rear area protection.
c. Administration and manning of prisoners of war cages.
d. Control of stragglers and refugees.
e. Protection of Main Supply Route (MSR).
f. Participate in infantry operations when necessary.
g. Manning of observation posts.
h. Route reconnaissance and surveillance.

5. **Battlefield Circulation Control**. The main battle mission of Military Police is Battlefield Circulation Control (BCC), it expedites the forward movement of combat resources. BCC ensure combat personnel, equipment, and supply move smoothly, quickly and little interference on Main Supply Routes (MSRs). MP control circulation on the battle field to meet changes in tactical situations and route conditions. The Battlefield Circulation Control includes the following:

a. Route reconnaissance and surveillance.
b. MSR regulation enforcement.
c. Straggler and refugee control.

6. **Route Reconnaissance and Surveillance**. As part of the BCC mission, MP conduct route reconnaissance to obtain detailed information on routes and on the nearby terrain from which the enemy can influence movement on the routes. MP continually monitors the condition of the MSR and ensure that the route is free of enemy's activities. The MP also seeks and report on routes which may be used as alternative route in case the MSR becomes inaccessible.

7. **Protection of Main Supply Route**. To keep the MSR free for re– supply operations, it must abide by the command's highway/route regulation measures' which is part of circulation plan. That is the specific measure needed to ensure smooth and efficient use of the road network, which include among others direction of travel, highway regulations, and MP traffic control post. Most important to the MP, that it gives it the control on classification of routes. The MP also ensures that the MSR is free of the movement of refugees and stragglers.

8. **Stragglers and Refugee Control**. Military Police performing battlefield circulation control mission also help

stragglers return to military control. Mobile patrol, traffic control post and checkpoint teams help stragglers as part of their day to day operations. Most stragglers are simply persons who have become separated from their command by events on the battlefield. MP directs these able bodied stragglers either to their parent units or to a replacement unit as command policy dictates. If stragglers are ill, wounded or in shock, MP gives them First Aid and then have them moved to the nearest facility. In other instances, MP escort apprehended stragglers back to their command, to a replacement unit (if any) or to a confinement center if their detention must continue.

9. **Information Dissemination**. As part of battlefield circulation control measures, military police personnel provide information particularly about the MSR, number of stragglers and refugees.

10. **Rear Area Protection**. Military police perform rear area security duties which entail forming all round defence of the rear area, screening of refugees and stragglers. The MP also deploys troops at Observation Post (OP) and patrol duties to ensure that the enemy does not carry out infiltration operation against the rear troops.

11. **Area Reconnaissance**. As part of their area security mission, MP units conduct area reconnaissance to guard against the unexpected enemy attack in the rear area. They watch likely enemy approach and landing or drop zones to give early warning of rear area enemy activity. MP seeks specific information about towns, ridgelines, forests, or other features from which the enemy can influence movements on MSR. MP pay close attention to areas near depot terminals, critical points, special ammunition supply points, communication centres and command and control HQ.

12. **Enemy Prisoners of War Collection and Evacuation Operation**. MP mission is of humane as well as tactical importance. MP performs their PW operations to collect and evacuate PWs from the battle area. At times, entire units of enemy forces could be separated and disorganized as a result of combat shock which might lead to their capture. MP receives PWs and civilian returnees from combat units as far forward as possible and the provost commander evacuate PWs promptly to the rear such PWs from the combat unit to the Div Admin Area (DAA). The MP must ensure that they protected and treated humanely.

ARREST

13. Arrest is the taking and restraining of a person from his or her liberty in order that he or she shall be forth coming to answer an alleged or suspected crime or offence levelled against him or her. Arrest can also be defined as deprivation of a person's liberty by legal authority, taking under real or assumed authority custody of another for the purpose of holding or detaining him to answer a criminal charge or civil demand or the moral or physical deprivation or restraining of a person's liberty. In military law, it refers to both open and close arrest.

POWER OF ARREST AND ARREST WITHOUT WARRANT

14. By virtue of the provision of Sect 315 of the 1999 Constitution, legality is provided for the enforcement of existing laws hence the derivation of power making the AFA. Sect 121 of the AFA CAP A20 LFN 2004 provides that persons subject to Military Law found committing offence under any provision of the Act or alleged to have committed an offence may be arrested in accordance with the provision of AFA. The Act also empowers the use of reasonably necessary force in affect an arrest. The power of arrest vested on a person by virtue of Sect 121 of AFA may be exercised either

personally or by ordering into arrest the person to be or by giving orders for that person's arrest.

15. Sect 10 of Criminal Procedure Act(CPA) and Sect 26 Criminal Procedure Code (CPC) empowers a police officer to effect arrest of an offender or any person who commits an offence, or reasonably suspected of having committed an offence. Sect 12 of CPA and Sect 28 of CPC, provides for a private person or citizen to effect the arrest of any person who in his view commits an indictable offence or who he reasonably suspects of having committed an offence. This can be done without warrant. It then means that this wide power of arrest by a private person is equally conferred and can be exercised by members of the armed forces. Any person may arrest in any of the following circumstances:

a. If there is a warrant or who he is directed to arrest by a Justice of Peace under 29 CPC or by superior officer section 30 CPC.

b. Any person who escaped from a lawful custody.

c. Any person required to appear by a public summon published.

d. Any person committing an offence in his presence, offences for which that police are authorized to arrest without warrant.

CONDITIONS THAT WARRANT ARREST

16. The following conditions will warrant an arrest:

a. When the offence carries a serious punishment.

b. When the accused undermines discipline.

c. When accused is likely to injure himself.

d. When accused is likely to interfere with witness and Investigation.

POINTS TO CONSIDER BEFORE EFFECTING ARREST

17. The following points should be noted before effecting an arrest:

a. Offence committed.
b. Types of arrest.
c. Conditions that will warrant arrest.

ESCORT

18. Provost Officers are frequently called upon both in peace and war time to provide escorts for high ranking officers, civilians, or convoy movement. Escort means the act or means of accompanying person(s) or valuable goods in order to protect or safe guard them to and fro or to their destinations. There are 2 types of escort duties:

a. Ceremonial escort.
b. Protective escort.

CEREMONIAL ESCORTS

19. Ceremonial escorts are usually provided for high ranking officers or civilian of equivalent status. It entails adequate preparation. Having mapped out the route to be followed, the escort commander will bear the following in mind:

a. **Planning**. Planning should include the following:

(1) Suitability of the rendezvous, final destination and reception arrangement, which have been given in the order for the escort.

(2) Trouble spots on the route such as factory sites (including opening, closing and meal times) Traffic lights, level crossings, road works and any other factor which may affect the timings of the movement.

(3) Possible emergency parking places enroute.

(4) Local geography and unit location, so that any last minute change in plan can be catered for.

(5) Confirm emergency refuelling and recovery arrangement.

(6) Methods or alternative means for communicating the progress of the movement.

(7) Police units located along the route must be informed of the details of the escort and adequate liaison carried out in case of assistance where necessary such as manual control of traffic, positioning of point men in towns, crowd control, use of one-way streets etc.

b. **Rehearsals and Reconnaissance**. Dry runs should be conducted to ensure timings and speeds. It is important that a further reconnaissance be carried out on the route shortly before the escort takes place. This is to ensure that no new obstruction or difficulties arose after the initial reconnaissance.

c. **Inspection of Vehicles**. Ensure that all escort vehicles are thoroughly checked by EME well before time of the escort and with particular attention to slow running.

PROTECTIVE ESCORTS

20. All the preparatory point noted for ceremonial escorts are applicable to protective escorts. Others areas to consider include:

a. **The Vehicle**. Police Vehicles will be stripped of canopies. Side screens and the windscreen will be lowered to the horizontal position. In certain circumstances armoured side screens may be used.

b. **Arms and Ammunition.**

(1) Drivers will be armed with pistols but the pistol case will be left unbuttoned.

(2) Other members of the escort will be armed with assault rifles. All weapons are to be loaded with the safety catch at safe position, while the muzzle points upwards at an angle not less than 45 degrees.

(3) All members of the escort must have attained a high degree of skill at arms and must have practiced firing from a moving vehicle.

(4) Orders for the control of fire must be clear and thoroughly understood by all members of the escort.

c. **Communications.**

(1) Protective escorts should have direct link by radio where applicable.

(2) Signal between drivers must be rehearsed as in the case of ceremonial escorts which include such additional signals to cover the halt, and execute turn round.

21. **Escort to Awkward Loads.** The movement of large nuclear weapons, tank transporters and other awkward loads can cause traffic congestion and will frequently require escorting. The escort should be mounted on motorcycle which is ideally suited for shepherding duties, due to their ability to pass through narrow areas.

22. **Conduct of the Escort**. The aim of the escort is to move the vehicles to be escorted as quickly as possible to their destinations without loss of life, disturbance to the flow of traffic or damage to property. The type and strength of the escort depends on the duty and distance to be covered.

SEARCH TECHNIQUES AND CLEARANCE PROCEDURE

23. Search simply means to look carefully in order to find something or somebody. In this context, search connotes looking at everything in a person's pockets and examining his or her body and clothes to see if anything of evidential value is concealed therein. It also means looking for any evidence in a vehicle, building or an area. Techniques refer to methods, means or act of performance. Clearance on the other hand means an official approval for something to go ahead or to be done. It also implies that a person, object, building or areas is certified to be blameless or secured. Procedure is the series of systematic actions that must be completed in order to achieve something. Search and clearance are systematic actions taken to certify person, vehicle, object or an area blameless or secured.

PRINCIPLES OF SEARCH

24. The following are the principles of search:

a. There must be reasonable grounds for the search.

b. The cooperation of the suspect must be sought.

c. The object and grounds for search must be explained to the suspect.

d. The extent of search must depend on article suspected.

e. A reasonable attitude must be used towards the suspect.

f. Juveniles and the handicap may usually be stopped and searched.

g. The outcome of the search (evidence) must be recorded in the presence of the suspect.

TYPES OF SEARCH

25. A search may be directed to people, object, building or an area. It will always involve both civil and military personnel since misuse of search authority can adversely affect the outcome of operations against dissidents, terrorists or suspects. Searches must be carried out properly if the outcome is to be of evidential value in a court of law. Proper use of search authority could gain respect and support of the people. Abuse, excessive or inconsiderate search technique may temporarily suppress the terrorists or expose some of them, but at the same time, such methods may ultimately switch civil populace sympathy and support to the terrorists. There are basically 4 types of searches. These are search of an individual, vehicles, house and an area.

26. **Search of an Individual**. Search must be tactful to avoid making an enemy out of a suspect who may, in fact, support the government/loyal troops. It is during the initial handling of persons about to be searched that the greatest caution is required. During the search of an individual, one member of the search team must always cover another one who makes the actual search. Usually, 3 techniques are adopted for individual search namely; frisk, wall and strip searches.

a. **Frisk Search**. Frisk is a quick search of an individual for weapons, evidence, or contraband. It is conducted preferably in the presence of an assistant and a witness. In conducting the frisk, the searcher stands behind the suspect. The searcher's assistance takes a position from where he can guard the suspect with his weapon. The suspect is required to raise his arms. The searcher then slides his hands over the individual's entire body, frisking the clothing to locate any concealed objects.

b. **Wall Search**. Based on the principle of rendering the

suspect harmless by placing him in a strained, awkward position, the wall search affords the searcher a degree of safety. It is particularly upright surface or a wall, vehicle or tree may be utilized.

c. **Strip Search**. Strip search is usually considered necessary when the individual is suspected to being a terrorist/leader or his important messenger. The search is conducted in an enclosed space such as a room or tent. The searching techniques can be varied. One method is to use two armed searcher with an assistant carefully. A search is then made of his persons, including his mouth, nose, ear, armpits, and other areas of possible concealment. It is therefore recommended that a female searcher must search a female suspect.

27. **Search Techniques**. In taking his initial position, the searcher must be alert to prevent the suspect from sudden attempt to disarm, or injure him. The search then checks the suspect's hands, arm, right side of the body and right leg in sequence the same procedure is repeated in searching the left side. He frisk the suspects clothing between his fingers. He pays attention to armpits, back, waist, tops of boot or shoes. Any item found that is not considered a weapon or evidence is placed in the suspect's pocket. A terrorist group/revolutionary force will make maximum use of females for all types of tasks where search may be necessary. To contain this, maximum use of female searchers or in the alternative a medical doctor is necessary.

28. **Search of Vehicles**. Vehicles are best searched in an area close to checkpoints. When searching a vehicle, all occupants are made to get out and stay clear of the vehicle. The driver should be made to observe the search of his vehicle. An assistant always covers the searcher. The occupants of the vehicle could be searched

simultaneously if sufficient searchers are available. A systematic search could be essential whereby parts of the vehicles are divided for easy search. The parts are inside the boot, interior, engine compartment and underneath.

29. **Search of Built-Up Area**. Search techniques must be perfected by counter – revolutionary force in populated areas. These techniques are required for searching either a few isolated huts, buildings or well-developed urban sections. The techniques to be adopted are as follows:

a. The area to be searched is divided into zones and search party is assigned to each. This party should at the minimum consist of a search element to conduct search, a security element to encircle the area and prevent entrance/exit and secure open areas and a reserve element to assist, as required.

b. Search of each zone must be conducted using personnel and other trusted devices considered necessary for the success of the search.

30. **Houses**. When it is decided to search inhabitants in one central area, the head of the house himself or herself is firstly searched. If this is not done, the head of the house is in a position to deny knowledge of incriminating materials found or could make accusation of theft and looting against troops. Buildings are best searched from bottom to top. First search moveable objects before the immovable ones in clockwise direction. Mine detectors are used to search for arms and ammunition. Every effort is made to avoid unnecessary damage. After searching a house containing property but without occupants, the house should be secured and a sentry placed outside to prevent looting.

SEARCH AIDS AND EQUIPMENT

31. Since the object of search is to find something of evidential value or to certify that an individual, object or place is blameless or secured, certain aids and equipment are necessary to carry out the task. The most important aid is the eyes. Other aids include the sense of smell, taste and feeling. The use of trained dogs is also helpful in search tasks. In order to enhance search and save time, some equipment are used. The search equipment are flash light, handheld metal detectors, multidimensional CCTV etc.

CLEARANCE

32. When the principles of search and its techniques are jointly applied to an individual, object or an area, and no incriminating evidence is found, a clearance certificate is then issued to the individual. However, it is important to note that clearing does not amount to blanket certification. For example, if an individual is to be blameless after a search, it does not mean such a person is cleared indefinitely. In fact, the individual could be arrested if there is a strong suspicion on his conduct.

33. Search and clearance procedure is an important aspect of security. In this period where world peace and security is under serious threat, security matters must not be taken for granted. Search and clearance procedures are the series of actions taken to find items of evidential value. In carrying out search, the correct type and technique must be applied using the aids and equipment readily available. Successful searches are those, which unearth information required, accepted in evidence, assist the government in gaining conviction in the law courts and reinforce the public confidence in the government's ability to keep the peace and security of its citizens.

GUARDROOM PROCEDURE

34. When a military Policeman makes an arrest, the offender will be taken to the guardroom where the following procedures will be followed:

a. On arrival at the guardroom, the accused will be handed over to the desk NCO for confinement.

b. The desk NCO fills in details of the handing over and committal receipts form.

c. The person authorizing the detention will complete the committal receipt proforma and sign.

d. Provision will be made for the welfare of the detainee.

WHEN NOT TO ACCEPT AN ACCUSED IN GUARD ROOM

35. A guard commander must not accept detainees in custody under the following conditions:

a. When the unit is to relocate or move within 24hrs.

b. When the guardroom is filled to capacity c When the unit has an outbreak of a contagious/ epidemic disease.

d. When the detainee needs medical attention.

e. When the person authorizing the detention has no powers to do so.

f. When the person is a civilian and not subject to Military law.

36. One of the ways the police enforce law and order is arrest and detention of culprits. When a suspect is apprehended and detained, it becomes easier for the police to carry out detailed investigation devoid of interruption. Thus, knowledge of guardroom procedure is very important to investigators so as not to violate the fundamental rights of the accused person who is presumed innocent until proven otherwise by a competent court. This is provided for by Sec 36 (5) CFRN 1999.

SPECIMEN OF HANDING OVER RECEIPT (CFB A6009)

Army No:..... Rank:..... Name: .....
Unit:..... Corps/Regt:..... Sign: .....
I was the guard commander on ..... when at ..... hrs, the above named soldier was handed over to me to be detained by ..... of .....
Army No:..... Rank:..... Unit:..... Date:..... Sign:.....

STAFF OF DUTIES ROOM

37. A standard military police duty room consists of 7 NCOs as follows;

a. Visiting NCO - Sgt.
b. Desk NCO - Cpl.
c. Guard room commander - Cpl.
d. 3 x IS Standby NCOs - Cpl and Lcpls.

DUTIES OF THE VISITING NCO

38. A visiting NCO is a Military Police soldier of the rank of SSgt/Sgt who takes charge of soldiers detailed on duty at the unit duty room. He has under command a Desk NCO who is a Cpl and 3 standby NCOs. He reports to the duty officer when the need arises. His duties are as follows:

a. He takes charge of all soldiers on duty at the unit duty room. That is, the desk NCO, guard room commander and IS standby soldiers.
b. He receives complaints and directs actions to be taken accordingly.
c. He visits all guard locations both by day and night and reports to ASA when the need arises.
d. He checks books in the duty room to ensure that entries are made correctly.
e. He ensures the safety and welfare of the detainees in the guard room.

LIMITATIONS OF VISITING NCO

39. There are limitations on the duties of a visiting NCO. They include the following:

a. The V/NCO has no right to send any of his NCOs out of his AOR to effect an arrest without the consent of his commanding officer.

b. He has no right to issue arms to his NCOs in the discharge of any assignment.

c. He must not take unilateral decision. He must contact his OC/ CO before acting on issues considered to be very serious.

THE DESK NCO AND FUNCTIONS

40. The desk NCO is a Military Police personnel below the rank of a sergeant in every provost unit, and the duties they perform include the following:

a. His tour of duty is from 0600hrs to 0600hrs the next day.

b. He is responsible for the security of the duty room both day and night.

c. He records all occurrences in the appropriate books.

d. He is responsible to the V/NCO and normally takes orders from him.

e. He receives complaints/records and transmits same to the V/NCO.

f. He keeps the keys to the exhibit room where detainees belongings are kept.

DUTIES OF UNIT RSM

41. RSM is an appointment given to the most senior warrant officer in a unit or formation. He serves as a link between the CO and his soldiers in a battalion, regiment or

formation. He is often addressed as the father of the unit or formation. His duties are as follows:

a. He is the link between the soldiers and the CO.

b. He is in charge of unit regimentation, sanitation and physical security.

c. He directs young officers on unit regimentation.

d. He supervises the regimental police of the unit.

e. He briefs the CO on general administration problems of the unit.

f. He is the patron of WOs and Sgt Mess.

g. He visits the guardroom to check detainees.

h. He visits the arms and ammunition stores to make sure they are properly maintained.

i. He conducts rehearsals with officers on sword drill.

j. He is in charge of unit quarter guard.

BOOKS MAINTAINED IN THE DUTY ROOM

42. The MP duty room is not meant for detaining suspects alone but also valuable items such as exhibits and detainees' properties are kept within the duty room. Thus, for proper documentation and accountability, books are maintained to account for such items accordingly. The Desk NCO maintains books and makes necessary entries in them. The various books maintained in the duty room are:

a. Daily occurrence book (DOB).

b. Detainees property book.

c. Exhibit book.

d. Telephone book (TB).

e. Detainees Book (DB).

f. Vehicles In and Out Book (VIOB).

g. Absentee and deserter index for MP only (AFB6510).

h. Criminal property book.

i. Early call book.

j. Arms Movement Register.

ROAD TRAFFIC ACCIDENT

43. Traffic is the movement of people, vehicles and animals on roads, ships, canoes on the sea and aircrafts. Accident on the other hand is the collision or similar incident involving a moving vehicle, resulting in property damage, personal injury or death. Since the invention of automobiles, human involvement in accident has increased out of proportion. It is important then to look for ways of arresting the situation before it gets out of hand.

MP ACTION AT THE SCENE OF RTA

44. Accidents occur often and on our roads. They could be a result of collision between vehicles or vehicle and animal or even a permanent object. They can as well occur between military vehicles and as a result MPs are called to cover the scene and the accident. Accident scene attracts sympathizers who offer to provide assistance to the victims. On reaching the scene of an accident, the following actions are to be carried out:

a. Attend to the injured and give first aid.

b. Call for ambulance if necessary.

c. Inform the civil Police.

d. Before the ambulance takes the injured or casualty away, obtain the particulars of the injured, obtain FMT3 and give to the injured person. If this is not possible due to seriousness of injury, enquire from the driver of the ambulance the hospital the injured is to be taken to.

e. Establish traffic control at the scene of accident to ensure smooth flow of traffic.

f. Take particulars of witnesses starting with civilians in case of civil vehicles

g. Make out sketch of the accident in the AB 466

h. Enter the details of the vehicles involved including drivers and passengers.

i. Note any land mark, traffic signs etc as a reference

point in order to pin point position of vehicles and persons involved.

j. Note the prevailing road and weather condition as at the time of accident.

k. Inform the Unit, relatives, property owners affected.

l. Remind the driver to complete his FMT3.

m. When the civil Police arrive at the scene, handover to them if the vehicles involved are civil vehicles but remain at the scene until the scene has been completely cleared.

n. Write a report covering the accident.

o. If occasion warrants you to carry out the duties of civil Police, this will require a follow up action through obtaining statements from witnesses.

DOCUMENT AND OFFICE SECURITY

45. Document of security is a term used to describe those security measures designed to ensure that classified documents are correctly safeguarded at all times. Document of security covers a wide range of items, notes, maps, photographs, slides, view foils, recorded taps, printing plates, etc.

BASIC RULES OF DOCUMENT SECURITY

46. The basic rules of security of documents are:

a. Documents should be classified correctly.

b. Classified documents should be kept to minimum handling.

c. Ensure that all documents are easily traceable.

d. Ensure that checks will reveal losses.

e. Prevent unauthorized access.

f. Ensure that staff knows the rules.

THE TEN RULES OF DOCUMENT SECURITY

47. Document security measures are based on the following 10 rules:

a. Each document is to be accorded with a security classification based -on the estimated damage.

b. Each document should be clearly marked with a security classification which correctly reflects its security value and indicate the appropriate standard of protection it will be given.

c. Classified documents are not to be accessible to any unauthorized person at any time. Access is to be restricted to those that need to know its contents in order to carry out their official function.

d. Each document should be properly recorded and controlled in such a way that the location of such document is known at all time.

e. Classified document must be transmitted in most secured ways only

f. When contents of a classified document are less important, the document should be downgraded and declassified accordingly.

g. Classified document are always to be stored under proper arrangement.

h. Under secured arrangement, classified document without needs, should be destroyed.

i. Classified documents are to be checked constantly not only at regular interval, but also at snap basis

j. If classified documents cannot be found or compromise is suspected, investigation should be conducted.

PRINCIPLES OF DOCUMENT SECURITY

48. The basic principle guiding the handling of security documents are as follows:

a. **Need to Know**. Since access to classified document is restricted to as few persons as possible, no person should be given more information than he/she needs to enhance his/her duties. Vetting clearance does not confer an automatic right of access to classified information.

b **Need to Hold**. Sometimes an individual may have the need to know the content of a classified document, but may not need to retain such document. One should only be allowed to retain classified information that is essential to his/her performance of duties.

c **Need to Take**. Although, someone may have need to know and the need to hold, only when there is real need that the document should be removed from the office.

OFFICE SECURITY

49. Offices are custodian of vital information that the Hostile Intelligence Service (HIS) tends to penetrate using so many means to execute bad plans. Thus, counter measures aimed at preventing unauthorized persons or intruders access to classified information are made by security officers of the organisation.

50. Espionage can be conducted in various ways, but the greatest threat is via unauthorized access, the offices should be adequately supervised to ensure that only tested and trusted persons have access to classified document. Technical measures must be employed to counter technical devices of stealing information or espionage. While documents are given adequate protection, photocopying should be done under supervision and control. Classified information and their biproducts should be all treated as classified information.

METHODS OF ESPIONAGE IN OFFICES

51. The following are methods of espionage:

a. Authorized access.
b. Third party with access.
c. Surreptitious means.
d. Negligence.
e. Technical eavesdropping.

CONTROL OF ACCESS AND PRECAUTION TO COUNTER EAVESDROPPING OF EQUIPMENT

52. Control of access to information is done by centralizing all classified information/document to a place; this will give ability to control its access easily. Those without authorized access would be denied entry to such places. Files passed to various offices should be locked away if the users stay away from the office temporarily. Offices should be properly cleaned up, technically swept and secured just before any conference.

53. The following are suggested precautionary measures to reduce or eliminate ability of (HIS) from bugging our offices:

a. Using anti metal devices at the gate to check and prevent unauthorized persons from bringing in recording/bugging equipment.
b. All keys should be treated as security keys.
c. Cleaners, redecorators/maintenance should be supervised.
d. Records of job done should be maintained.
e. Records of workers should be maintained.
f. Inspection of equipment/furniture before and after removal, for repairs, should be done.
g. Visitors without permission should be escorted.

PRECAUTIONS FOR COMMUNICATION AND ELECTRONIC EQUIPMENT IN OFFICES

54. Installation of electronic or communication equipment requires the services of security agencies in the provision of security. Electronic typewriters are not very safe for classified documents. The ribbon and carbon used shall be given adequate protection. Classified by products could be easily traceable too. The use combination locks and key control system is vital in office security.

55. **Combination Setting (Locks)**. Combination of locks setting should be changed at the following period:

a. When a container is first brought to use.
b. On posting of combination set order.
c. At least once in every 6 months.
d. When compromise is suspected.
e. After repairs and inspection.

56. **Key Control**. The following rules are recommended for good key control

a. Minimum number of keys should be used (one key to one door).
b. Protect keys from unauthorized eyes.
c. Centralized and secure storage, duplicate or triplicates keys.
d. Issue key on signature.
e. Use security key register.
f. No key should be removed from unit without absolute need.
g. Keys should be changed every six month.

HOME SECURITY

57. Family security tips are centred on making individuals home safe. Thus, protecting your home and family from criminal intrusion

should be high on your list of priorities. The greatest problem to security is to presume that there is no threat in your area. When criminals are to attack their victims, they apply the principle of surprise. Therefore, the use of burglary proof and other devices is very important to deter criminals from visiting.

DEVICES FOR HOME SECURITY

58. There are many devices that could be used for home security. Some of the devices are:

a. Burglary proof.

b. Doors and locks.

c. Sliding glass patio doors.

f. Lighting.

d. **Windows**. The following steps could be taken to ensure that your window is secured:

(1) Secure all accessible windows with secondary blocking devices.

(2) Block accessible windows open no more than 6 inches for ventilation.

(3) Ensure that someone cannot reach through an open window and unlock the door.

(4) Ensure that someone cannot reach inside the window and remove the blocking device.

(5) Use anti-lift devices to prevent window from being lifted out.

(6) Use crime prevention or alarm decals on ground accessible windows.

e. **Good Neighbour**. Things to note about neighbourhood:

(1) Get to know all your adjacent neighbours,

(2) Invite them into your home and establish trust.

(3) Agree to watch out for each other's home.

(4) Do small tasks for each other to improve territoriality.

(5) While on vacation - pick up newspapers, and flyers.

(6) Offer to occasionally park your car in their driveway.

(7) Return the favour and communicate often.

HUMAN SECURITY

59. Human security is a post-cold war multi-disciplinary approach that grew out of a number of different researches, including development studies, international relations, strategic studies and human rights. According to a UNDP report, human security consists of 2 basic pillars: the freedom from want and the freedom from fear. This means the absence of hunger and illness as well as of violence and war despite so many criticisms. The term remains appealing because it acknowledges the inter-relatedness of a variety of factors that contribute to individual well-being.

60. Human security is the part of physical security that deals with economic, food, health, environmental, personal, community, and political security for the protection of individuals and its well-being in the society.

TYPES OF HUMAN SECURITY

61. Human security is all encompassing and has to do with our daily endeavours. For a better understanding, human security is broken down into several aspects. The following are the types of human security:

a. **Economic Security**. Economic security requires an assured basic income for individuals – usually from productive and remunerative work or in the last resort from some publicly financed safety net. In this sense, only about a

quarter of the worlds people may at present be economically secured while economic security problem may be apparently more serious in developing countries, same concern also arise in developed countries.

b. **Food Security**. Food security requires that all people at all times have both physical and economic access to basic food. According to the UN, the overall availability of food is not a problem rather the problem often is the poor distribution of food and a lack of purchasing power.

c. **Health Security**. Health security is aimed at guaranteeing a minimum protection from diseases and unhealthy lifestyles. In developing countries the major causes of death are infections and parasitic diseases, which kill many people annually. Most of the deaths are linked with poor nutrition and unsafe environment (particularly polluted water). In advanced countries or industrial countries, the major killers are diseases of circulatory system causing millions of deaths in a year.

d. **Environmental Security**. Environmental security is aimed at protecting people from short and long term ravages of nature, man made threats in nature and terror action of the natural environment. In developing countries, the greatest environmental threat is that of water. Water scarcity is increasingly becoming a factor in ethnic strife and political tension. Water pollution also leads to the lack of safe sanitation in developing countries. In developed countries, air pollution is the major threat.

e. **Personal Security**. Personal security involves individual protection against physical violence, whether from the state or external states, violent individuals, sub-state actors, domestic abuses predatory adults etc. In many societies, human lives are at greater risk than ever before. For many people, the greatest source of anxiety is crime

especially violent crime.

f. **Community Security**. Community security protects people from loss of traditional relationships and values, and from sectarian and ethnic violence. Traditional communities, particularly ethnic groups come under much more attack from each other.

g. **Political Security**. Political security assures people live in a society that honours their basic human rights. According to survey by Amnesty International, political repression, systematic torture, ill-treatment or disappearance was still practiced in over 100 countries. Along with repressing individuals and groups, governments may try to exercise control over ideas and information.

h. **Collective Security**. The philosophy of collective security has been propounded throughout history on grounds of morality, divine will or economic and social utility. Collective security evolved in the 19th century, when the modern search for a means of preventing war began with the rise of nation-states at the end of the Middle Ages. Following the First World War, the hopes of many pacifists for achieving collective security were directed toward the newly formed League of Nations. This organization was loosely constructed and provided no really effective means of preventing war. By 1941 most of the nations of the world were involved in Second World War. This was followed in turn by the establishment of the UN, with its more elaborate machinery for keeping the peace.

SCHOOLS OF THOUGHT OF HUMAN SECURITY

62. Human beings seek security for so many reasons. These could be classified under 2 schools of thoughts:

a. **Freedom from Fear**. This school seeks to limit the practice of human security to protecting individuals from

violent conflict. This approach argues that limiting the focus to violence is a realistic and manageable approach towards human security. This approach is also called humanitarian or safety of peoples approach. Emergency assistance building prevention and resolution, peace-building are the main concerns of this approach.

b. **Freedom from Want**. According to UNDP 1994, 'freedom from want school of thought focuses on the basic ideal that violence, poverty, inequality, diseases and environmental degradation are insuperable concepts in addressing the root of human insecurity different from "freedom from fear" it expands the focus beyond violence with emphasis on development and security goals. Japan for example, has adopted the broader "Freedom from want" perspective in its own foreign policy and in 1999 established a UN trust fund for the promotion of human security.

63. An application of human security is highly relevant within the area of humanitarian intervention as it focuses on addressing the deep rooted and multi-factorial problems inherent in humanitarian crises, from war and mass murder to natural disasters and famines often occur in the absence of economic and socio political system, that provide infrastructure for adequate access to the basic needs and rights that make people feel secure in their environment.

PHYSICAL SECURITY

64. Physical security plan is a comprehensive written document providing proper and economical use of personnel and equipment to prevent or minimize loss. Adequate planning also prevents damage, misuse, espionage, sabotage and other criminal or disruptive activities. Failure of physical security plan of an installation could jeopardize or expose the facilities of the installation to the ills of intruders.

65. Physical security is the first line of defence and it is geared towards achieving the following:

a. Inhibiting theft and vandalism.
b. Controlling the environment.
c. Limiting access to system components.
d. Restricting access to backup tapes.

PHYSICAL SECURITY TERMINOLOGIES

66. The following physical security terminologies should be well understood and use correctly. They are:

a. **Installation.** An installation is a grouping of facilities, located in the same vicinity, which support particular functions.

b. **Restricted Area**. A restricted area is an area in which special security measures are employed to prevent unauthorized entry. Restricted access plan is often based on the following:

(1) National emergency.
(2) Disaster.
(3) Terrorist or hostile threat.
(4) Significant criminal action.
(5) Civil disturbance.
(6) Other contingencies that would seriously affect the ability of the installation to perform its mission.

c. **Security Lighting**. Security lighting is designed to deny an intruder approaching the area the cover of darkness and enable personnel at the facility to detect unauthorized personnel within the area.

d. **Physical Security Inspection**. Physical security inspection is a formal assessment of physical procedures and measures implemented by the organization to protect, preserve and maintain its assets.

e. **Security Policy**. Installation commanders or security officers must develop, plan and maintain policies that could ensure effective installation access control. The policies should:

(1) Determine the degree of control required over personnel and equipment entering or leaving the installation.

(2) Prescribe and distribute procedures for the search of persons (and their possessions) on the installation.

(3) Enforce the removal of, or deny access to persons who threaten order, security or discipline of the installation.

(4) Designate restricted areas to protect classified defence information or safeguard property or material for which they are responsible.

d. **Survivability**. The ability to withstand or repel an attack or other hostile actions to the extent that essential functions can continue or be resumed after the hostile action. The survivability of a security guard could be improved using the following measures:

(1) Provide a 20-foot clear zone on the inside and outside of the perimeter barrier. All underbrush in the clear zone should be removed and all depressions and raises should be levelled. (2) Prohibit personnel from parking vehicles within 30 feet of perimeter.

(3) Bury fuel storage tanks and fuel lines for back-up generators underground.

(4) Bury power and communications cables underground.

(5) Maintain an emergency water supply and store it underground.

(6) Elevate air-conditioning systems at least 12

feet above the ground.

(7) Paint buildings and essential structures in toned-down colours, such as light green, light brown and other earth shades.

(8) Install hardened defensive fighting positions that cover probable avenues of approach by hostile elements.

ATTRIBUTES OF SECURITY FORCES

67. Security forces/personnel are to be of high moral standing. Their disposition should be tactful and they must possess full mental alertness. Other attributes are:

a. Alertness.
b. Good sense of judgement.
c. Confidence.
d. Physical Fitness.
e. Tactfulness.
f. Self control.
g. Mental attitude.
h. Responsibilities and trustfulness.

CRIME DETECTION

68. The responsibility of law enforcement agencies is to detect crimes, apprehend the perpetrators, and provide evidence that will convince judges that the perpetrators are guilty beyond reasonable doubt. To accomplish these, several methods are used, including reconstructing the crime, collecting physical clues, and interrogating suspects and witnesses. Essentially, the methods of detection employed by investigator are dictated by the nature of the crime and the procedures permitted by the legal system.

EARLY METHODS OF CRIME DETECTION

69. Early criminal investigation was a crude process, relying on

eyewitnesses, inferences, informers and confessions extracted under torture. Other methods of crime detection which are still useful in criminal investigations are:

a. **Surveillance**. Surveillance is one of the oldest ways of detecting criminal activity. This method is used when it is likely that a crime will take place at a specific location or when certain persons are suspected of criminal activity. Surveillance techniques may include placing personnel in strategic locations and equipping them with optical aids or electronic devices, sensitive to pick conversation from a considerable distance.

b. **Interrogation**. Interrogation is used when the information sought is not readily forthcoming, perhaps because of hostility or guilt of the suspect. An investigator must apply the logic of reasoning or interrogative techniques to obtain useful information from suspect.

Criminal Records. Criminal records represent an important data base for police activities throughout the world. A special branch of records called intelligence files contains biographical information on selected criminals. These files include criminal specialties, associates, and skills and other information that might suggest future criminal involvement and the means by which the criminals can be apprehended. Records are also used for a general analysis of crime, so that police administrators can be informed of criminal trends and the best ways to suppress them.

SCIENTIFIC METHOD OF CRIME DETECTION

67. Scientific investigation, forensic science or medical jurisprudence is regarded as the application of science to law. Forensic science uses highly developed technologies to uncover scientific evidence in a variety of fields. Modern forensic science can help law-enforcement officials determine whether any laws or regulations have been violated in various fields of human

endeavour. It can also determine whether automobile emissions are within a permissible level and whether drinking water meets legal purity requirements.

USE OF FORENSIC SCIENCE IN CRIME DETECTION

68. Forensic science is most commonly used to investigate criminal cases involving firearms, body fluids, poison etc. Forensic scientist conducts investigation in the following areas:

a. **Examination of Firearms**.
Firearms are identified through microscopic imperfections that are produced inadvertently in gun barrels during manufacture. A bullet fired from a pistol or rifle, has impressed on its surface the individual characteristics of the barrel through which it was fired. The firing pin, breech face, extractor, and ejector come in contact with the cartridge case; hence, cartridge cases may be scarred with distinctive markings that can be identified with a particular gun.

b. **Serological Investigation**. Serology is the study of body fluids in relation to sickness and its treatment. In crime detection, serological procedures are applied to the identification of a blood stain to determine its human or animal origin and its blood group classification.

c. **Toxicological Investigation**. Toxicology could be defined as the science of poisons. Special methods of analytical chemistry have been developed for use in toxicological examinations. The specimens ordinarily examined in cases of suspected poisoning are tissue samples from vital organs, blood or urine, food, drink, and the suspected poison itself.

d. **Hairs and Fibres Examination**.
A piece of hair or a few strands of fibre when compared with known specimens may prove valuable in solving a case. A fibre found on a cut screen at the scene of a

burglary may be associated with a suspect's jacket, or a hair found on a suspected car in a hit-and-run case may help prove that the car struck the victim.

e. **Mineralogical Investigation**. The science of mineralogy is also used in crime detection. The mineralogist studies soil, plaster, cement, brick, concrete, and glass for any evidence. Soil and dust found on a suspect's clothing and determined to be comparable to that at the crime scene help to prove the person's presence in that locality.

f. **Metallurgical Examination**. Metallurgical examination makes it possible to identify the source of an item—whether made of metal, plastic, ceramic, or other material found at a crime scene. Metallurgical examinations can also determine how a metal item was manufactured, and whether items found in different locations were made at the same time and by the same manufacturer. Such identification helps trace the evidence to its owner.

g. **Document Examination**. Document examination consists largely of comparing disputed or questioned handwriting with known handwriting to determine the writer's identity. It includes the examination of hand printing, forgeries, typewriting, inks, and related items. Writing process is so complex that personal peculiarities always persist in the handwriting of any given individual.

h. **Odontological Examination**. Forensic odontologist examines the characteristics of the teeth of unidentified bodies when fingerprint or other identification is not available. The dental charts of missing individuals can then be compared with the forensic odontologist's report to identify the body. Investigators can identify a body by comparing old X rays and the medical history of a

missing person with the findings of the forensic anthropologist.

TECHNIQUES OF FORENSIC SCIENCE

72. Some techniques used for forensic science are:

a. Alcohol Test.
b. Gas chromatographyor blood test.
c. Use of microscope devices.
d. Fingerprint.
e. Deoxyribonucleic Acid (DNA).
f. Odontological examination.
g. Coroner inquest.

IMPORTANCE OF CRIME LABORATORY

73. Forensic laboratory in criminal investigation provides a conducive atmosphere and convenience for the investigator. With the scientific items and reagents, tests are carried out on samples obtained from the crime scene, victim of crime, criminal and/or his/her environs to help prove a crime to a logical conclusion. Forensic laboratory is important based on the following reasons:

a. It assists the field investigator to clear ambiguities during investigation.
b. It links criminal with the crime scene.
c. It corroborates or disproves alibi.
d. It provides expert testimony.
e. It provides for expert training.
f. It exonerates the innocent.

ISSUES AFFECTING CRIME LABORATORY

74. A crime laboratory may be faced with series of issues. Some of these issues include:

a. Improper way of collecting/handling evidential sample from the crime scene by the field investigators.

b. Lack of knowledge on capability of the laboratory.
c. Distance between location of labs and other formations.
d. Lack of trained personnel for the laboratory.
e. Lack of maintenance.

POLICE ACTION AT THE SCENE OF CRIME

75. A crime scene technician or police officer on arrival must ensure that the scene is protected for easy crime scene investigation or crime scene processing. To protect the crime scene, the police officer must dominate the scene; provide guard to prevent unauthorized persons from gaining entry into the crime scene. Essentially, prompt and early arrival of police officer at the crime scene would ensure that witnesses are identified, evidence protected and culprits arrested if possible.

76. The action of a police officer at the scene of crime is very crucial to the welfare of the victims and successful completion of the case. At the scene of crime, a police officer is expected to carry out the following action:

a. Provide First Aid treatment to victims.
b. Arrest of perpetrators.
c. Protection of the crime scene – The protection of crime scene can be done through the following:
    (1) Disperse the crowd or persons not related to the case.
    (2) Provide guard to prevent entry of unauthorized persons and exit of witnesses.
    (3) Protect evidence such as finger or foot print, blood stain, broken glasses, hairs and fibres.
    (4) Protect object used in the commission of the crime.

d. Record Information.
e. Brief the Investigator.

CRIME SCENE PROCESSING

77. Crime scene processing is a complicated and multiple tasking functions. Each crime scene is different and may require a different approach to processing the scene. However there is a basic crime scene procedure that should be adhered to in all crime scenes. These basic procedures are as follows:

a. **Interview**. The first step in processing a crime scene is interview of persons within and around the crime scene. The crime scene technician must interview the first officer at the scene or the victim to ascertain the "theory" of the case. This information may not be factual information but it will give the crime scene technician a base from which to start his investigation.

b. **Examine the Scene**. Examination of the crime scene is the second step in crime scene processing. Examine the scene to ascertain if the information gathered on the case is substantiated by what the crime scene technician observed.

c. **Photograph**. Photographing the crime scene is the third step in crime scene processing. Photographing crime scene is aimed at recording pictorial view of the scene and to record items of possible evidence. Crime scene photographs are generally taken in 2 categories; the overall view and items of evidence.

d. **Sketch**. Sketching the crime scene is the fourth step in crime scene processing. A rough sketch is completed by the crime scene technician to demonstrate the layout of the crime scene or to identify the exact position of a deceased victim or evidence within the crime scene. A crime scene sketch may not be completed on

every case.

INTERVIEW AND INTERROGATION OF SUSPECTS

78. An interview is the questioning of a complainant, victim, witness or suspect who is willing to provide information that would be of interest to the investigator. During the interview, little or no motivation for the witness needs to be supplied by the investigator. The witness is merely encouraged to tell what occurred. Questions are asked only when witness leaves out pertinent facts or makes valuable statements.

79. The information needed to further an investigation must be obtained from people who have some significant knowledge concerning the crime. Witnesses or victims are interviewed, and suspects are interrogated. Interrogation is used when the information sought is not readily forthcoming, perhaps because of hostility or guilt. Often, some key to the solution of a crime, such as the location of the weapon in a murder case, is known only to the perpetrator. Without information provided by the suspect or informant, a crime may go unsolved.

USES OF THE INTERROGATION PROCESS BY THE MILITARY POLICE

80. The essence of arresting, interrogating and prosecuting a criminal is to bring him to justice so as to achieve individual and general deterrence in the society. The purpose of interrogating a suspect is to achieve the following:

a. To extract information that the accused person would not otherwise disclose willingly.

b. To determine the guilt of a suspect and his level of involvement (principal offender, accessory before or after the fact and accomplices).

c. Doubt created by the accused person, witnesses or even the complainant could be addressed through interrogation.

d. An accused person could be linked with the exhibit he/she concealed or dropped before arrest through interrogation.

e. As part of control measure used by the police to prevent crime, receivers of stolen items, criminal hideout and sources of weapon could be uncovered through interrogation.

f. Victims of past operation of criminal gangs could be disclosed through interrogation for possible recovery of stolen items.

g. A well conducted interrogation produces a true confession, which has a powerful impact on a criminal case.

ABUSES OF INTERROGATION PROCESS

81. The police abuse of interrogative process is a term used to describe excessive use of physical force, assault, verbal attack, threat by investigator to elicit information from suspects. When a suspect confesses to achieve freedom from torture or discomfort, such confession cannot be admitted in a court of law. Similarly, when an investigator convinces an innocent person that he or she is guilty of a crime he or she could not remember committing; such admission of guilt is void. Other forms of abuses of interrogation process are:

a. Use of tear gas and powder gas on the faces of suspects during interrogation.

b. Hanging and torturing of suspects in an interrogation room.

c. Maiming of suspects using hot iron or pliers to

remove their finger nails.

d. Cocking of rifle, firing into the sky or close to an accused person before commencing interrogation.

e. Crawling on hot stone, frog jumping, denial of food and sleep.

f. Killing of suspects on the pretext that they attempted to escape.

PSYCHOLOGICAL TECHNIQUES OF EXTRACTING FACTS FROM CRIME SUSPECTS

82. The complexity of human nature or behaviour makes it very difficult for investigators to extract facts from crime suspects without applying force. This is because suspects would not ordinarily give statements that would incriminate them. However, psychologists have developed some techniques that could be applied to extract facts from suspects without the use of force. Some of these techniques of extracting facts from a crime suspects are:

a. Establishment of Good Rapport.
b. Assurance of Confidentiality.
c. Clarification by the Suspect.
d. Questioning the Suspect.
e. Restatement by the Investigator.
f. Probing by the Investigator.
g. Psychological Profiling.
h. Overt Observations.

WHY SUSPECTS DO NOT CONFESS AND WHY THEY DO

83. Criminal justice administration requires a systematic approach to criminal reports through the use of procedures and appropriate investigation methods, reliable procedures and techniques. Obtaining information and facts about a given crime

from a suspect, eye-witness, informant, terrorists, prisoner of war, spy, espionage and other security or anti security agents is one of the most difficult tasks in criminal investigation. Thus, investigators are often tempted to employ unconventional to extract information from unwilling suspects.

84. Crimes must be properly investigated in order to:

a. Uncover any hidden fact about a given crime which would subsequently help in identifying the suspects and accomplices involved.

b. Collect crime information that would lead to understanding the nature and pattern of crimes in the society.

c. Collect information that will assist security agents to control.

d. Collect information that will lay claims to criminal charges and subsequent passing of judgments by the courts.

WHY SUSPECTS DO NOT CONFESS

85. Interrogation and interviews are very difficult tasks which deal with encouraging the suspects to confess even when they known that such confessions will lead to their loss of freedom or lie due to the gravity of the offence. This explains the unwillingness and resistance to confess which can be as a result of the following:

a. Fear of going to jail.

b. Fear of being killed or suffering bodily harm from a co-defendant. for instance in a case of fraternity.

c. Fear of losing one's job, business or pension.

d. Fear of losing one's professional license such as medical, legal etc.

e. Fear of losing one's life style.

f. Reluctance to involve a loved one.
g. Fear of embarrassing family members.
h. Reluctance to give up the fruits of the crime.
i. Fear of opening up the door to other crimes they have committed.
j. Suspect has been told by a lawyer not to confess.
k. Reluctance to involve co-defendants.
l. When a suspect is convinced that there is insufficient evidence to get a conviction.

PSYCHOLOGICAL REASONS WHY SUSPECTS DO NOT CONFESS

86. Suspects could on account of psychological reasons fail to confess to the investigator for the following reasons:

a. Bad interrogation environment such as too many people around.
b. When suspects do not trust the interrogator.
c. When a suspect does not want to experience the shame of being guilty.
d. When a suspect has pride of not losing his manliness.
e. When a suspect does not want to give up his weapon of revenge.
f. When the case is a claim to fame and he enjoys the celebrity status that could be diminished by an admission of guilt.
g. When a suspect has an overriding ego which he would not want to destroy by admitting guilt.
h. When a suspect has been a prolific liar all his life.
i. When the interrogator has the facts wrong, the suspect would not confess unit he gets them right.
j. When a suspect is masochistic in nature even when a confession would be to his advantage.

l. When a suspect is enjoying, the role as victim of an alleged injustice as the falsely accused rather than the perpetrator.

m. When a suspect does not want to give his adversary a victory by confessing (business partner, wife, rival etc).

n. When a suspect is trying to hide his ignorance and by lying becomes the smartest one in the room because he knows the truth which the interrogator does not.

o. When a suspect does not remember the precise details of the crime possibly as a result of the influence of drugs, alcohol or time.

p. When a suspect is embarrassed by the crime because he possesses an expertise that should exclude him from such minimal acts.

q. Suspect committed a benevolent act during the crime that, in his mind negates his guilt.

WHY SUSPECTS CONFESS

87. The ultimate aim of interrogation is to elicit voluntary confessions which are often hard to achieve even among hardened. This explains the need to have sufficient background training and experience in the area of psychology and communication. Modern psychology has revealed that the stimuli in every interview situations can be manipulated to create demand characteristics which the suspects instinctively reacts to. It is assumed that under the weight of unfamiliar environment coupled with fear and anxiety imposed by the interview environment, the suspect will be willing to confess his or her offence in order to be relieved of his or her continuing guilt, fear and emotional suspense. Willingness to confess can be grouped into the following categories:

a. **Practical Reasons Why Suspect Confess.** Suspects confess because of the following reasons:

(1) When suspect realizes that there is too much evidence against him.

(2) To get a lesser penalty, better deal or become a witness rather than a perpetrator.

b. **Psychological Reasons Why Suspects Confess.** Suspects confess because of the following psychological reasons:

(1) When suspect is institutionalized and has no fear of going to prison. Most times happier inside than out.

(2) When confessions are obtained by torture.

(3) When the suspect is worn-out by a long period of interrogation and would want the interrogator off his back.

(4) When confession is meant as revenge or to embarrass a loved one.

(5) When there is sensual feelings and pride in the crime committed.

(6) When the suspect is a masochist who would prefer to confess in order to insure punishment.

(7) When the confession is made in an effort to gain personal and public interest, respect and acceptance.

(8) When the suspect succumbs to the entreaties of his family.

(9) When the act is so bizarre that the suspect is hoping that someone else will give him insight as to why he did it.

(10) When there is the influence of religious teachings.

(11) When there is the desire to relieve the conscience of such traumatic issues.

HOW SUSPECTS LIE TO INVESTIGATORS

88. **Use of Loophole Remarks, Statements and Expressions**. Liars have only one strategy in mind, which is to convince the interrogator that they are telling the truth. Thus, they employ certain tactics and make predictable statements. It has been established that liars react the same way using the same loophole remarks and expressions. Some loophole statements, remarks used by suspects are:

a To the best of my knowledge.
b Not that I remember.
c. Not that I'm aware.
d. Not that I can think of.

89. **Use of Over-Sell Expressions by Suspects.** Over sell expressions are used by suspects. These expressions are designed to add more weight to what follows them and to make that more believable. Liars find it difficult to respond with a simple "yes" or "no". To appear credible, they always add some of the following expression:

a. Honestly.
b To be honest
c. Truthful.
d. Frankly.
e Believe me.
f. If I'm lying, may I drop dead.
g. I swear to God.
h. I swear on my mother's grave.
i. If I'm lying, may my wife and children burn in hell.

90. **Thinking Time Statements**. One of the obvious signs of lying is that the person hesitates before responding to a direct question. The reason is simple; you have to think before you lie. Thinking-time statements are interjections before the response is made. In that sense they differ from loophole statements, which is the response. Examples of thinking time statements are:

a. Who, me?
b. What was that question again?
c. Can you repeat the question?
d. I don't understand the question.
e. What did you say?.
f. Are you asking me that question?
g. Uh/Uhmm.
h. Why should I have to answer that, it was a long time age.
I. Do you want me to tell you the truth?

91. **Brooklyn Bridge Remarks**. Some remarks are both comical and abusive to the investigator. They indicate that the suspect is between not confessing and confessing. They are made by people who are trying to work up the nerve to confess. Expression such as:

a. I didn't steal the money, but I feel morally obligated to pay it back.
b. I need to know if I did it.

92. **Offence Statements**. These statements are made by design to put the interrogator on the defensive. In making these statements, the suspect tends to take control of the interview. If the interrogator doesn't answer these questions in a forceful manner he's in trouble. The interrogator can regain dominance by telling the suspect precisely why the suspect asked the question. Point out to the suspect that he asked the question as

an evasive tactic and to avoid the responsibility of giving a direct answer to the question. Such statements are:

a. Why should I lie?
b. Do you want me to tell a lie on myself?
c. Are you accusing me?
d. Are you calling me a liar?
e. Why would I do anything like that?
f. Are you trying to put words in my mouth?

93. **Tactics**. Tactics in lying emanate from defence mechanisms. Essentially, defence mechanisms are instinctive and are necessary ingredients in the evolutionary process. They are a means of avoiding acceptance of one's wrong doing. The defence mechanisms that you encounter most frequently in any interrogations session are projection, disassociation, rationalization, and identification. Almost all of the tactics employed by liars are encompassed by 4 defence mechanisms:

a. **Projection**. Displacement of blame outside oneself to another or to society in general.

b. **Disassociation**. Thinking-away process; compartmentalizing of the mind to exclude guilty thoughts. Both actions are a conscious effort to enhance denial.

c. **Rationalization**. Giving nice reasons rather than real reasons to save face. It's been my experience that people justify an act at the time it's committed or that they seek justification later to make the act tolerable.

d. **Identification**. Attributing moral characteristics to oneself that would preclude the individual from committing any wrong doing.

THE PROBLEMS FACING INVESTIGATORS IN THE MILITARY POLICE

94. Investigation is an official examination of facts about a situation, crime etc. The act of investigation is a cumbersome one that requires aptitude, tact and great deal of discipline for one to successfully arrive at a logical conclusion. The MP has investigators who are specially trained to carry out these tasks. However, the MP investigator experiences some problems in the course of carrying out his duties. Some of these problems are integral to the investigation process while others are as a result of lapses in the system.

PROBLEMS FACING THE MP INVESTIGATOR

95. The problems confronting the MP investigator in the course of discharging his duty are so numerous. However, some of them are highlighted as follows:

a. Inadequate training.
b. Inadequate equipment.
c. Paucity of funds.
d. Lack of regimentation.
e. Inability to attend civil courses.
f. Hasty demand of investigation reports.
g. Supervening interests in a case.
h. Attitude of investigators towards informants.
i. Absence of consistent mobility.
j. Integrity.

CRIMINAL INVESTIGATION

96. The essence of investigation generally is to uncover secrets which are of special importance somewhere. Investigation of any kind may not necessarily follow if something secret is not at stake. Criminal investigation is therefore, an art and not a science. In practice, it is better to assume that criminal

investigation is a science. As a body of science, it is complete with general principles, special theories and hypothesis. If the investigator adopts them, it will enable him reach valid conclusion about the case under investigation thereby finding it much easier to solve crime. But where he fails to apply these and takes to unorthodox methods, he is bound to fail in the cases he is investigating.

DETECTIVE'S WORKING PHILOSOPHY

97. Most detectives develop a working philosophy based on the following:

a. No two crimes are alike.
b. Most crimes are solved in 48 hours.
c. Most crimes are solved by guess work and luck.
d. The law provides guidelines as to what happened.
e. The mode of operation provides clues as to who is responsible.
f. Criminals always make mistakes.
g. Evidence is always present.
h. People always lie to you.
i. Learn to work with others.
j. Know when to give up.
k. Public opinion is important.
l. You can never receive too much training.
m. Think like a 'native' not a criminal.
n. Document everything.
o. Establish credibility in court.
p. The correct culprit is to be put behind bars, but not by any means.

TYPES OF CRIMINAL INVESTIGATION

98. The different types of investigation can be classified as proactive and reactive, or as covert and overt:

a. Proactive (Covert).

b. Reactive (overt).

99. A proactive investigation is usually covert (secret) and a decoy (police posing as victim) or sting (police posing as buyers or sellers) operation. A reactive investigation is usually based on a citizen complaint, and involves a preliminary and follow-up (or latent) investigation. A preliminary investigation is the early reporting of all known facts, usually done by the patrol officer of first responder. A follow-up investigation is always done by detectives, and generally involves one of 3 activities.

a. **A Walk-through of the Crime Scene**. Not so much as to gather evidence, but to think about and refine one's theory about a specific suspect.

b. **Where are They (The Location of the Perpetrators)**. Here the detective uses sources of information to find the location of any and all the suspects.

c. **Who are They (The Identity of the Perpetrators)**. Here the detective is developing suspects from where there are none apparent.

100. Preliminary investigations are normally done by the first responder, usually the patrol officer, but there may be times when the detective is involved in a preliminary investigation. First responders should rush to the crime scene, and in doing so, should remain vigilant for any gateway vehicle or other suspicious things along the way. The first responder should assist in preservation of the crime scene, separation of witnesses, and requests for warrants.

101. The acronym PRELIMINARY summarizes most of the duties expected at preliminary investigation:

P – Proceed to scene promptly and safely.
R – Render assistance to injured person(s).
E – Effect arrest of the criminal.
L – Locate and identify witness.
I – Interview complainant and witnesses.
M – Maintain integrity of crime scene and protect evidence.
I – Interrogate suspects as necessary.
N – Note condition, events and remarks.
A – Arrange for evidence collection.
R – Report the entire incident full and accurately.
Y – Yield responsibility to follow-up investigators.

Follow up investigation usually begins by reading over all the original reports and paperwork, and looking for leads. There are 6 major pieces of police paperwork involved in a follow up investigation:

a. **Synopsis**. A cover page showing a table of contents and a suggestive list of which pieces of evidence make the strongest case for the prosecution.

b. **Summary of Facts**. A short one or two paragraphs description of the crime committed by the perpetrator.

c. **Police Paperwork**. All police forms and reports, starting with the incident report to the supervisory review report but leaving out until later any lab or crime scene notes.

d. **Testimonial Statements**. The transcripts, video, or audio of any interrogation and the arranged statements of any witnesses or others interviewed or contacted along with an evaluation of what they will testify to and what they may not testify to.

e. **Record Checks**. The rap sheet, bank statements, or printout from any sources of information done on the backgrounds of principal parties to the case.

f. **Crime Scene Information**. Photographs, sketches, notes and a summary of all evidence collected, processed and analyzed, including any expert analysis or criminality reports. Any coroner or medical examiner's report goes in the back of the dossier (file) as an appendix.

DEFINITION OF TERMS

102. Crime detection, apprehension of offenders as well as prosecution of criminal are the statutory roles of criminal investigation. This implies that apprehending criminals to face the wrath of the law could serve as deterrence in our society. It is important for all provost personnel to be familiar with certain terms used in criminal investigation. Some of the terms are as mentioned below:

a. **Crime**. A crime is a legal wrong. It is an act or omission which renders the person doing the act or making the omission liable to punishment under the law.

b. **Criminal**. Any person who does the act or makes the omission which constitutes a crime is known as a criminal.

c. **Investigator**. Investigator includes all the police officers who are empowered to work, search or inquire into a complaint or allegation with the aim of establishing the truth of the matter.

d. **Investigation**. This is the act of collecting and examining facts to accomplish the three fold aims of – identifying, locating the guilty party and providing evidence of guilt in any court of competent jurisdiction.

e. **Informant**. A person who gives intelligence or

information to the police is known as an informant.

f. **Informer**. A person who gives information or one who informs against another is known as informer.

g. **Interrogator**. This is a person who asks questions in order to ascertain position of an event or incident.

h. **Criminal Investigation**. The criminal investigation comprises those tasks or actions by law enforcers be it private or public. In the criminal investigation, there must be an incident that is capable of including crime that is something very unpleasant to both the victim and the bearer or observers and in fact, all within that vicinity. This is something that affects the law of the land.

AIM AND OBJECTIVES OF CRIMINAL INVESTIGATION

103. The basic aim of criminal investigation is to determine the culpability of a suspect after uncovering the secrets which are of special importance somewhere or otherwise of the innocence of an accused person. It is important to locate the where about of the criminals, arrest them and bring them to book. Likewise, criminal investigation has the following objectives:

a. **To Identify the Suspect**. This is the first stage of criminal investigation. The identity of the suspect can be identified by the following ways:

(1) Confession.

(2) Eye witness testimony.

(3) Circumstantial evidence.

b. **To Locate or Trace the Suspect**. This is the second objective of criminal investigation. It is therefore, very important that the perpetrator must be located. In most cases, the criminal is not hiding, but he is simply unknown.

c. **To Prove the Guilt**. This is often the most difficult phase. It involves gathering the facts necessary in the trial to prove the guilt of the accused beyond reasonable doubt. It requires that guilt be proved beyond reasonable doubt and that the evidence be presented in a certain form and in accordance with a prescribed procedure and that it satisfies certain requirements of quality and trustworthiness.

d. **Presentation of Evidence in a Court of Competent Jurisdiction**. The final object of criminal investigation is the presentation of evidence in a court of competent jurisdiction. The fact of the existence of crime must be established and linked to the accused person who must be identified and associated with the crime scene. Competent and credible witnesses must be available.

STEPS OF THE INVESTIGATIVE PROCESS

104. Criminal procedure governs the investigation of crimes; the arrest, charging, and trial of accused persons. This implies that when a case is assigned to an investigator, he/she must follow the steps of scientific method of investigation process to bring the perpetrators to justice. The steps an investigator will take depend on the types of criminal investigation. The steps an investigator will take in a proactive investigation are quite different from the steps he will take in a reactive investigation. The following are steps in investigative process to be taken by an investigator for thorough and speedy case file compilation:

a. Determine if a Crime Has Been Committed.
b. Verify Jurisdiction.
c. Discover all Facts and Collect Physical Evidence.
d. Identify the Perpetrators.
e. Recover Stolen Property.
f. Provide Evidence in Court.

g. Testify as Prosecution Witness in Court.

105. Criminal investigation has the end product of bringing someone to justice. The enormous responsibility of proving the guilt of the accused person calls for strict adherence to the steps of investigative process. An Investigator must know the steps he/she should take from the moment a case is assigned to him till the final determination of the case in court.

CASE FILE COMPILATION

106. Criminal cases reported to MP have to be investigated. The investigation of criminal case is also known as case file compilation. A case file contains all facts and evidences about complaints or reports made to the police which have become a subject of investigation. A case file comprises of the following:

a. A case file jacket.
b. The index to the case file.
c. Extract from the dairy.
d. Police report.
e. Minute sheet.
f. Statement of complainant(s), accused person(s) and documentary exhibits.

107. A case file should be arranged in the following order:

a. Index to case file.
b. Extract from crime dairy.
c. Investigation report.
d. Minute sheet(s).
e. Letter of authority.
f. Statement of complainant.
g. Statement of witness(es).
h. Statement of accused or suspect(s).
i. Other documentary evidence.

108. The file jacket should contain the following information:

a. Case number.
b. Station.
c. Offence.
d. DOB entry number.
e. SIB/Unit crime diary number.
f. Name, address, nationality of complainant.
g. Name, address, nationality and age of suspect.
h. Name, address, nationality and age of deceased (if any).
i. Date, time and place of offence.
j. Date, time reported to NACMP.
k. Value of property stolen, destroyed or recovered.
l. Name of officer in-charge (investigator).
m. Exhibit recovered (if any).
n. Date suspect was arrested and by whom.
o. Date suspect released on open arrest.
p. Date accused was finally released.
q. Date investigation was completed.
r. Date case was forwarded to unit.
s. Date case was sent to civil police.
t. Result of trial or inquiry.

SEQUENCE OF INVESTIGATION REPORT

109. Criminal investigation report writing has a format and sequence that must be followed by investigators. The sequence is as follows:

a. Address of investigators unit.
b. Addressee.
c. Subject.
d. Reference(s)
e. Suspect(s).

f. Basis for investigation.

g. Allegation.

h. Investigative summary - Facts required in investigative summary are; invitation of complainant to write his statement including dates and invitation of suspects and witness for statement including dates. It also requires other activities such as searches, visit to crime scene either before or after.

I. Substantiation – Substantiation should cover a brief introduction of the complaint, introduction of the suspect and elements of Proof of the offence. It should also focus on the corroborative evidence and exonerate those not found culpable.

k. Conclusion.

l. Recommendation.

INTERIM REPORT WRITING

110. Criminal investigation report requires statements of all parties concerned. However, when an investigator could not arrest and record the statements of the suspect(s) or principal witness(es), an interim report could be written and forwarded to Appropriate Superior Authority (ASA). The essence of interim report is to intimate the ASA on the case under investigation. Interim report serves the following purposes:

a. To brief ASA on the actions taken by the investigator.

b. To brief ASA on the problems encountered by the investigator during the course of the investigation.

SEQUENCE OF INTERIM REPORT WRITING

111. The sequence of interim report writing is as follows:

a. **Introduction**. The investigator must write a brief introduction of the case as against the basis of

investigation and allegation. However, all facts related to basis of investigation and allegation must be stated in the introduction.

b. **Findings**. Findings of the case uncovered during investigation should be itemized.

c. **Hindrances or Problems Encountered**. Interim report is not a conclusive report because of certain problems encountered by the investigator. Such problems should be stated in this paragraph. The essence of this paragraph is to prompt ASA into action.

d. **Opinion**. The personal or expert view of the investigator must be expressed. For example where the principal suspect is on foreign course or operation, the opinion of the investigator could be either to wait until the suspect returns or request for his repatriation.

e. **Recommendation(s)**. The recommendation is based on the opinion expressed.

JOINT INVESTIGATION WITH CIVIL POLICE

112. The civil police would always request for the release of service personnel for interrogation when involved in criminal activity. In such situation, the Commissioner of Police (CP) writes to the GOC, Bde Comd or CO of the soldier. But if the soldier was arrested by the civil police, the CP writes the unit of the soldier to inform his comd. Both instances require the Provost Comd to initiate a joint investigation as follows:

a. Identify the soldier and apprehend him.

b. Allow the civil police investigators to interrogate the soldier together with your investigators.

c. Follow the police to their station to interrogate the soldier's gang members if any.

d. If the soldier is in police custody, visit the station and identify the soldier.

e. Carry out joint investigation to establish the guilt or other wise of the soldier.

f. Request for the soldier's release for regimental trial if he is guilty and if he is not guilty, you release him.

g. Try the soldier for conduct prejudicial to service discipline and not the substantial charge of armed robbery.

h. Hand him over to civil police to face civil prosecution.

IMPORTANCE OF JOINT INVESTIGATION

113. The importance of joint investigation are as follows:

a. Accused persons are given fair trial.

b. Police abuse of interrogation process is minimized.

c. Promotes inter services cooperation and understanding.

d. Ensures proper dismissal of accused persons from the Service.

e. Allows civil police to investigate service personnel involved in criminality.

f. Allows civil police to investigate wards of Service personnel involved in criminal act.

VETTING OF A CASEFILE

114. Whenever a report is made either orally or in writing to any constituted authority, it is required that, such a report be investigated and be prosecuted if a prima facie case has been established against any person found to have breached the law. When a case is to be investigated, a case file is opened by the military police. It is important to note that a well structured and detailed case file is more often likely to contain facts identified during investigation. Poorly put together case file are often

returned by the appropriate superior authority if such case files do not meet an acceptable standard. All case files, no matter how trivial the case investigated is are highly confidential documents and must be secured at all times.

115. **Security of a Case File**. Case file should be properly secured by the investigating officer either in his office locker or under the custody of his supervising officer or under the prosecuting officer at the court level. Case file should not be allowed into the hands of an unauthorized person since it is both an official and confidential document. The loss or missing of any case file is at the risk of the investigating officer who handles the case file with poor security. No case file should be carried home by the investigating officer as movement with case file may meet mishap.

116. **Vetting**. Vetting of a case file or case dairy is the discreet examination of a case file or case dairy in order to detect mistakes made by investigating officer or his superior and to direct the investigating officer to rectify such mistakes. Such mistakes that normally occur in case file during investigation include:

a. Failure to follow up information by complainant/witnesses.
b. Mistake in the section of the offence committed.
c. Failure to clear alibi by suspects.
d. Failure to execute search warrants.
e. Failure to endorse and countersign statements.
f. Failure to date statements.
g. Failure to file important documents.
h. Failure to register case file and exhibits, etc.

Vetting of case file exposes these mistakes and brings about their corrections, thus bringing a case file up to date.

117. The vetting officer while vetting should ensure the following:

a. Establish the elements of the offence committed from the extract made from the Crime Diary to ensure the correct title.

b. Read statements of parties and witnesses to ensure cohesive evidence for prosecution or refusal.

c. Establish all points to prove the charge or direct the investigating officer to establish the point.

d. Ensure the investigating officer contacted all witnesses mentioned.

e. Ensure that exhibits are recovered and properly registered.

f. Ensure that confessional statements by the offender are attested to by a senior officer ie administrative officer and alibis are investigated.

g. Ensure that the investigating officer filled the dairy of action and it tallies with dates.

h. Ensure previous minutes are complied with.

i. Never temper with statement of accused by underlining the statement as this may affect the prosecution in court.

j. Be definite in your instructions to the Investigating Officer (IO).

k. Clear all ambiguities detected during vetting by interviewing the parties personally.

ACTION AFTER VETTING

118. After vetting and all directives in the minutes are complied with in the case file, the following actions are taken by the senior officer:

a. If prima facie case is made against the offender, a

correct charge is preferred against him.

b. If there is no sufficient evidence to prove the alleged offence, the case file is to be closed accordingly on its own merit.

c. If the suspect cannot be arrested (seen) the case could be closed undetected.

d. If the report is found to be made with malice, the complainant should be charged for false information against the suspect.

METHODS OF VETTING CASEFILE

119. It is important that the vetting officer go through the vetting process in a logical manner. The following methods are valid:

a. Check the elements of the offence by reading the extract from the crime dairy against the title of the case file.

b. Read carefully the statement(s) of complainant and witnesses and ensure you understand them clearly.

c. Ensure that all points to prove the charge is present, if not, direct the investigator on the next thing to do.

d. See to it that all those named as witnesses to the case have been contacted and their accounts obtained and recorded. If any of them is omitted, find out why.

e. Where there are exhibits, they should be kept with the exhibits keeper and properly labelled.

f. Read the statement of the accused and witnesses carefully and ensures they are properly recorded.

g. Ensure confessional statement of the accused is endorsed by a superior police officer or make use of attestation forms.

h. Where a defence of alibi is put up by the accused, direct the investigator to cross-check it to a logical conclusion.

i. Read the minutes in the minute sheet and ensure that all previous instructions to the investigator had been carried out.

j. Check and regularize the following:

(1) Paging of the case file.

(2) Search warrant (if necessary).

(3) Doctor's report/post mortem examination report.

(4) Handwriting expert report.

(5) Ballistician report (if necessary).

(6) Any publication.

(7) Statements to ensure that they have been properly signed, translated if applicable, and unambiguous, etc.

k. Lastly, read the police investigation report by the investigator or team handling the case, as it is assumed by now that the officer vetting would have formed his opinion about the case and therefore cannot be misled by the investigator any more.

CASE FILE AND RECORDS DESTRUCTION

120. The following orders are made in regard to the period of time a case file shall be kept before destruction or disposal:

a. Case files pertaining offences, other than murder, which have been disposed of in court of law can be destroyed after 3 years.

b. Case files pertaining murder case which has been disposed off in a court of law and those pertaining to undetected offences other than murder can be destroyed after 5 years.

c. Case files pertaining to undetected cases of murder can be destroyed after 7 years.

PRISONER OF WAR

121. Prisoner of War status came into recognizance with the introduction of the law of war, which consists of international prescription on the conduct of combat, and the protection of the victims of combat. Within the armed forces it is the duty of every commander to ensure the detail execution of the law of war within his sphere of responsibility taking cognizance that enemy armed force captured are prisoners of war.

122. A prisoner of war is a member of enemy armed forces including volunteers, resistance group or any other person belonging to enemy power operating in or outside their own territory, and captured as a result of battle actions.

OBJECTIVE OF HANDLING PRISONERS OF WAR

123. The handling of captives of war by a capturing unit is based on the following objective:

a. Maximizing intelligence information.
b. Weakening the morale of the enemy.
c. Using prisoners as a source of labour.
d. Prevent escape or liberation.
e. Promoting proper treatment of likely captured own personnel.

PRINCIPLES OF HANDLING PRISONERS OF WAR

124. The following principles may apply in handling PW

a. Humane treatment.
b. Opportunity for PW's interrogation.
c. Prompt evacuation from the combat area.
d. Compliance with international agreement.

ACTION ON CAPTURING PW

125. The general procedure for processing prisoner include, search/tagging of PW material, reporting, evacuation, segregation and safe guarding. The sequence of actions is:

a. **Disarm and Search**. On capture PW, he will be disarmed immediately and search for hidden weapon, equipment and document of intelligence value e.g Maps tactical manuals, orders book, air photographs, code books. Personal effect such as helmet, badge of rank, identify cards are not to be taken from PW.

b. **Tag Materials Found on PW**. Personal effects of the PW, other materials like captured weapon, map, code numbers etc must be tagged for proper accountability. Tag must include information about the PW from whom items were recorded.

c. **Report**. When PWs are captured, report must be sent to the ASA for necessary action.

d. **Segregation and Service**. PW will b e segregated on capture. Officers will be separated from other ranks, while female PW will be separated from male.

e. **Evacuation**. PWs will be evacuated as quickly as possible from battle area to the rear. Maximum use of empty transports returning to the rear will be evacuated through medical channel and will be segregated too. The immediate evacuation of the PWS to the rear is to prevent any interference with tactical movements.

f. **Interrogation**. Interrogation of PW in the combat area is the duty of the intelligence personnel. It is necessary to interrogate PW immediately after capture for first hand information about enemy situations.

g. **Safeguard**. PW must be protected from any possible harm from battlefield and prevented from escape.

CATEGORIES OF PRISONERS OF WAR

126. PW are categorised into the following.

a. Officers – M/F.
b. Non-commissioned officers – M/F.
c. Privates.
d. Deserters.
e. Hostile individuals war zone.
f. People taking political sides.
g. Nationality by birth.

MILITARY WORKING DOG HANDLING

127. Dogs have been used to hunt for food, animals, guard livestock and property, pull carts, perform rescues, and apprehend lawbreakers. They have been used during wartime as sentinels and message carriers. Today, trained dogs are used to alert deaf people to common household sounds, such as the ringing of a telephone or doorbell; guide the blind; or retrieve objects for quadriplegics. One of the most common of the many roles carried out by domestic dog is the companion they give. As animals with strong social tendencies, dogs typically crave close contact with their owners.

128. Military Working Dogs (MWD) are any breed of dog trained in order to carry out assigned task of detecting crime, narcotics or arms and ammunition. MWDs are also trained to carry other tasks such as search and rescue operation, cadaver operation, bomb/IED detection amongst others.

TYPES OF POLICE DOGS

129. There are more than 300 breeds of dogs that exist worldwide. However, only few are trained as MWDs. This module will cover only 4 breed of dogs. These are:

a. **German Shepherd**. The German shepherd is trained for protecting sheep. It is also the single most popular guard and protector dog today and is also popular and often trained as a MWD.

b. **Rottweiler**. The Rottweiler despite its reputation for viciousness is one of the most popular breeds worldwide. The powerfully built Rottweiler is a solicitous and calm animal, and is used as a pet and guard dog. Adult Rottweiler could attain a weight of 41 to 50 kg.

c. **Doberman Pinscher**. The Doberman pinscher is a cross between the Rottweiler, the German shepherd. The Doberman is a typical breed known for its aggressiveness and good for guard duties.

d. **Labrador Retriever**. The Labrador retriever is one of the most popular companions and helper dogs as well as aggressive guard dog.

130. **Dog Communication**. Dogs communicate through their use of body language. Facial expression, ear posture, tail carriage, hackle (hair on back) display and body stance signal a dog's state of fear, excitement, aggression, or submission. Understanding the meaning behind these signals can be important signs of potential hostility. Dogs may also growl or bark. People observing these behaviours should keep their arms at their sides and slowly back away, while firmly saying "no". When approaching a strange dog, first ask the owner if the dog may be touched. Once given permission, hold the hands low and speak softly. Staring directly at a dog may arouse intimidation or aggression, so eye contact with strange dogs should be avoided.

131. **Training**. The decision to adopt a dog should be made carefully because it is a serious commitment that can last for several years. Small dogs may live 12 or more years, although

very large dogs typically have a shorter lifespan, sometimes as brief as 8 years. Training is a vital part of raising a happy and healthy dog. The first lessons should be relatively brief for about 10 to 15 minutes a day, and gradually increase to 30 minutes, depending on the dog's level of concentration. Training is best accomplished with lots of praise and a stern "no" for corrections.

EMPLOYMENT OF MWD

132. MWDs can be employed to carry out the following duties:
    a. Assisting the human masters in combating crime.
    b. Tracking of suspected, wanted or missing persons.
    c. Searching of building or vehicle for narcotics or weapons.
    d. For crowd control and dispersals
    e. For guarding of persons and premises.
    f. Search and rescue operations
    g. Cadaver operations.
    h. Bomb/IED detection.