NATIONAL OPEN UNIVERSITY OF NIGERIA

COURSE CODE :CSS241

COURSE TITLE: BASIC SECURITY AND SECURITY THREATS

COURSE GUIDE

CSS241 BASIC SECURITY AND SECURITY THREATS

Course Developer/Writer
Monsuru Adegboyega Kasali
Non-Violence and Intercultural Communication
Advocacy Initiatives, Ibadan, Nigeria

Course Editor
Rasidi Okunola, Ph. D
Department of Sociology
University of Ibadan
Oyo State

Course Coordinator
Adeniyi T. Adegoke, Ph.D
Criminology and Security Studies
School of Arts and Social Sciences
National Open University of Nigeria

Programme Leader
Prof. Abdul-Rasheed Yesufu
Dean, School of Arts and Social Sciences
National Open University of Nigeria

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
No. 5 Dar es Salam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Published by

National Open University of Nigeria

Printed

ISBN:

CONTENTS **PAGE**

Introduction

CSS 241: Basic Security and Security Threats is a 3-credit unit course. It is a compulsory course for all undergraduate students in the field of Criminology and Security Studies of the University. The course is also recommended to any other student(s) particularly those in the School of Arts and Social Sciences, who may have interest in the study and survey of security theory and practice. The course can also be taken as elective or required course by other students whose main field(s) of discipline is not Criminology and Security Studies. However, the Course consists of 20 units, which include the meaning and approaches to security, forms of security, simulation in security planning and management, natural and manmade threats to security, safety measures to the management of security threats, civil security, intelligence and counter intelligence, etc. In this study, security issues and policies in Nigeria and Africa are given special focus with the aim of stimulating effective knowledge of the overall security situations and agenda in Nigeria and Africa, among the students so that they can identify, analyse, and proffer solutions to security problems locally and internationally.

The course has no compulsory pre-requisites. The course guide informs us on what this course is all about, what the student should appreciate in each unit, what text materials will be used and how we can make best use of these materials. This course guide also emphasises the need for students to take tutored marked assignments seriously. However, necessary information on tutored marked assignments shall be made known to students in a separate file, which will be sent to each student at appropriate time. This course is also supported with periodic tutorial classes.

What You Will Learn in this Course

CSS 241: Basic Security and Security Threats as a course in the field of Criminology and Security Studies at the National Open University of Nigeria focuses on a wide range of issues concerning ways to effect basic security measures and policies and identifying various threats that can jeopardise the security of any people or community. In this course, we carefully analyse and assess security threats, to assist the student not only to identify these threats but also to develop diagnostic framework through which they can proffer solutions to hazard mitigation and effective security management. In this course, the student or reader will also be exposed to various measures that can safeguard the protection of life and property against the incidence of security threat and hazard.

Nevertheless, the essence of these safety measures is to provide the student or reader with various ways through which he/she can reduce losses from any incidence of hazard or security attack, if you cannot prevent such threat or hazard from occurring. Knowing the impact that active involvement of civilians in security process can have in complementing and increasing the capacity of the security personnel to carry out their duties effectively well, the course also explores the strategic importance of civil security and how it can contribute to effective security management and threat mitigation. However, the issue of intelligence is very germane in security planning and management. Due to this reason, it is not surprising to see a great number of countries expending huge resources in human and financial terms to fortify their intelligence security and infrastructure. And owing to the fact that security discourse cannot be complete without looking at the issue of intelligence, it is pertinent in this course to also discuss the subject (intelligence).

Thus, the course covers a wide spectrum of issues regarding security intelligence including meaning of intelligence, intelligence collection, to mention but a few. In this course, we shall complete our study by studying the importance of data mining and automated data analysis to crime prevention and detection, intelligence gathering, intelligence analysis, threat mitigation and the overall security management.

Course Aims

The overall aim of CSS 241: Basic Security and Security Threats as a course is aimed at introducing you to the basic meaning of security and basic ideas, methodologies and approaches in security management. It is also aimed to expose the student or reader to knowing most of the existing threats to security. This may be categorised into two: natural and manmade. The study also explores the meaning of other manmade threats i.e. information warfare, arms production and proliferation, as well as war, and how they pose a risk to any people or communities.

Undoubtedly, the way the course draws its references from Nigeria and Africa in the analysis of various security threats makes it astounding and thought-provoking. It will provide assist the student a pathway in the field of Criminology and Security Studies to develop deliberate analytical consciousness on the aspects of general security practice and management through which the student can develop viable frameworks in proffering solutions to security problems locally and internationally. The course is also aimed to:

- Identify basic security ideas and policy actions;

- Clarify various forms of security especially how they constitute basic security management;
- Describe the application of simulation in security planning and management;
- Conceptualise the term security threat;
- Categorise security threats;
- Discuss various types of major natural security threats;
- Examine various manmade security threats;
- Draw inferences on how information warfare, arms production and proliferation like war constitute security threats;
- Propose safety measures against both natural and manmade threats to security;
- Explore how civil security can advance effective management of security in any community;
- Provide operational definition or meaning of the term intelligence;
- Elaborate on the activities and processes of intelligence of collection;
- Illustrate the processes of intelligence analysis; and
- Stress the importance of data mining and automated data analysis to intelligence gathering, intelligence analysis, crime investigation, crime prevention and detection, threat mitigation as well as security planning and management.

Course Objectives

With utmost desire to achieve the aims set out above, the course has a set of objectives demonstrated in all the units of the course. Each unit has its own objectives. Objectives are included at the beginning of every unit to assist the student to appreciate what he or she will come across in the study of each unit to facilitate his or her better understanding of the course-CSS 241: Basic Security and Security Threat. Student is therefore advised to read these objectives before studying the entire unit(s). It is helpful to do so. You should always look at the unit objectives after completing a unit. In this way, you can be sure that you have done what was required of you by the unit. Below are the wider objectives of this course as a whole. By meeting these objectives, you should have achieved the aims of the course as a whole.
At the end of the course, you should be able to:

- Explain the meaning of security and its approaches;
- Identify basic security ideas and policy actions;
- Clarify various forms of security especially how they constitute basic security management;
- Describe the application of simulation in security planning and management;
- Conceptualise the term security threat;
- Categorise security threats;
- Discuss various types of major natural security threats;
- Examine various manmade security threats;
- Draw inferences on how information warfare, arms production and proliferation as war constitute security threats;

- Propose safety measures to the management of both the natural and manmade threats to security;
- Explore how civil security can advance effective management of security in any community;
- Provide operational definition or meaning of the term intelligence;
- Elaborate on the activities and processes of intelligence of collection;
- Illustrate the processes of intelligence analysis; and
- Stress the importance of data mining and automated data analysis to intelligence gathering, intelligence analysis, crime investigation, crime prevention and detection, threat mitigation as well as security planning and management.

Working through this Course

In completing this course, the student is required to study all the units, and try to read all (or a substantial number of) the recommended textbooks, journals and other reading materials including electronic resources. Each unit contains self assessment exercise(s) and the student is required to submit his or her assignment for the purpose of assessment. At the end of the course, the student(s) shall be examined. The time of the final examination and venue shall be communicated to all the registered students in due course by relevant school authorities or study centre management. Below are the components of the course and what you are required to do.

Course Materials

Major components of the course include:

1. Course Guide
2. Study Units
3. Textbooks
4. Assignments File
5. Presentation Schedule

It is incumbent upon every student to get his or her own copy of the course material. You are also advised to contact your tutorial facilitator, if you have any difficulty in getting any of the text materials recommended for your further reading.

Study Units

In this course there are twenty units, which include:

Module 1

Unit 1 Security: Meaning and Approaches
Unit 2 Forms of Security I
Unit 3 Forms of Security II

Unit 4 Forms of Security III
Unit 5 Simulation in Security Planning and Management

Module 2

Unit 1 Meaning and Types of Security Threat I: Natural Threats
Unit 2 Meaning and Types of Security Threat II: Manmade Threats
Unit 3 Information Warfare as a Security Threat
Unit 4 Arms Production and Proliferation as a Potential Threat to Security
Unit 5 War as a Security Threat

Module 3

Unit 1 Safety Measures to the Management of Natural Threats
Unit 2 Safety Measures to the Management of Manmade Threats I
Unit 3 Safety Measures to the Management of Manmade Threats II
Unit 4 Civil Security: Meaning and Approach I
Unit 5 Civil Security: Meaning and Approach II

Module 4

Unit 1 Meaning of Intelligence
Unit 2 Intelligence Collection and Disciplines
Unit 3 Intelligence Analysis and Evaluation
Unit 4 Counter-Intelligence
Unit 5 Data Mining and Automated Data Analysis

The first module consists of five units, which will expose the student or reader to the conceptual definition of security and various approaches to security studies and practice. In this set of units, we shall also examine different forms of security and the last area of discourse in this module is simulation in security planning and management. In this course, we shall dedicate the second module to explore some of the major threats to security. We shall begin our study in this module by explaining the meaning of security threat and then categorise types of threats. In order to further illuminate the subject (security threat), we shall be drawing inferences to show how such issues like information warfare, arms production and proliferation as well as war undermine the security of any people or community.

In the third module, we shall be focussing on various actions and processes through which we can safeguard our lives and property against hazardous incidents or threats/attacks. We are aware that our discourse on safety measures cannot be complete if we fail to discuss issues of civil security, which can help in building the capacity of the people, towards acting creatively and effectively to mitigate or reduce the losses that may accompany a hazardous incident or attack. Owing to the strategic importance of intelligence to security management, we shall be discussing wide range of issues about it (intelligence) in a few units. We shall do this by adapting the past works of the author for the same programme and university on the subject of intelligence. In furtherance of our knowledge on basic security and threat mitigation, we deem it necessary to shed light on the importance and application of data mining and automated data analysis to security operation.

Text-Books and References

The following textbooks are recommended to each student taking the course.

Alemika, E. E. O. (1997). Police, Policing and Crime Control in Nigeria. *Nigerian Journal of Policy and Strategy* 12 (1 & 2): 71 - 98.
Alemika, E. E. O. (1993). Colonialism, State and Policing in Nigeria. *Crime, Law and Social Change* 20: 189-219.

Dannreuther, R. (2007). *International Security: The Contemporary Agenda*. West Sussex: John Willey & Sons.

Kinkus, J.F. (2002). Science and Technology Resources on the Internet: Computer Security. *Issues in Science and Technology Librarianship*, No. 36. Available on ://www.istl.org/02-fall/index.html. Retrieved on 30 August, 2009.

Molander, R. C., Riddile, A. S. & Wilson, P. (1996). *Strategic Information Warfare: A New Face of War*. Santa Monica, California: RAND, MR-661-OSD.
Bar, M. S, (2005). West Africa: From a Security Complex to a Security Community. *African Security Review* 14 (2). Also available on ://www.iss.co.za/index.php?link_id=3&slink_id=1936&link_type=12&slink_type=12&tmpl_id=3. Retrieved on 3 December, 2009.
Shettima, K. & Chukwuma, I. (2002). Crime and Human Rights in Nigeria. Paper Presented at the International Council on Human Rights Policy Review Seminar, themed Crime: Managing Public Order in Countries in Transition. New York, 21-22 October.

Sutton, J. L. & Kemp, G. (1966). *Arms to Developing Countries: 1945-1965*. London: Institute of Strategic Studies.

Onyeozili, E. C. (2005). Obstacles to Effective Policing in Nigeria. *African Journal of Criminology and Justice Studies* 1(1): 32-54.

Tickner, J.A. (1995) Re-visioning Security. In: Booth, K. & Smiths, S. (eds.). *International Relations Theory Today*. Cambridge: Polity Press. 175-198.

Waever, Ole (1995). Securitization and Desecuritization. In: Lipschutz, R.D (ed.). *On Security*. New York: Columbia University Press. 46-86.

Wardlaw, G. (1989). *Political Terrorism: Theory, Tactics and Counter Measures*. Cambridge: Cambridge University Press (2nd Edition).

Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press.
Lipschutz, R. D. (ed.). (1995). *On Security*. New York: Columbia University Press.
Davies, P. H. J. (2002). "Ideas of Intelligence: Divergent National Concepts and Institution". *Intelligence*, Vol. 24 (3), Fall. Also available on .harvardir.org/articles /1064 131. Retrieved on 8th April, 2008.
Monahan, T. (ed.). (2006). *Surveillance and Security: Technological Politics and Power in Everyday life*, New York: Routledge.
Dory, A.J. (2003). *Civil Security: Americans and the Challenges of Homeland Security*. Washington DC: Center for Strategic and International Studies (September).

Assignment File

In this file, you will find the necessary details of the assignments you must submit to your tutor for assessment. The marks you get from these assignments will form part of your final assessment in this course.

Assessment

There are two aspects to the assessment of this course. First the tutor-marked assignments and second is there is a written examination. In tackling the assignments, you are expected to apply information and knowledge acquired during this course. The assignments must be submitted to your tutor for assessment in accordance with the deadlines stated in the Assignment File. The work you submit to your tutor for assessment will count for 30% of your total course mark. At the end of the course, you will need to sit for a final three-hour examination. This will count for 70% of your total course mark.

Tutor-Marked Assignment

There are twenty tutor-marked assignments in this course. You need to submit four assignments out of which the best three will be used for your assessment. These three assignments shall make 30% of your total course mark. Assignment questions for the units in this course are contained in the Assignment File. You should be able to complete your assignments from the information and materials contained in your set textbooks, reading and study units. However, you are advised to use other references to broaden your viewpoint and provide a deeper understanding of the subject. When you have completed each assignment, send it, together with TMA (tutor-marked assignment) file to your tutor. Make sure that each assignment gets to your tutor on or before the deadline. And in case of being unable to complete your work on time, contact your tutor or betterstill your study centre manager (overseer) before the submission deadline of assignments elapses to discuss the possibility of an extension.

Final Examination and Grading

The final examination of CSS 241 shall be of three hours' duration and have a value of 70% of the total course grade. The examination shall consist of questions which reflect the type of self-testing, practice exercises and tutor-marked problems you have come across. All areas of the course will be assessed. You are advised to revise the entire course after studying the last unit before you sit for the examination. You will find it useful to review your tutor-marked assignments and the comments of your tutor on them
before the final examination.

Course Marking Scheme

This table shows how the actual course marking is broken down.

Assessment	Marks
Assignment 1 – 4	Four Assignments are to be submitted, out of which the three best shall be considered at 10% each, making 30% of the overall scores
Final Examination	70% of overall course marks
Total	100% of course marks

Table 1: Course Making Scheme

Course Overview

This table brings together the entire units contained in this course, the number of weeks you should take to complete them, and the assignments that follow.

Unit	Title	Week's Activity	Assessment (end of Unit)
	Course Guide	1	
1	Security: Meaning and Approaches	1	Assignment 1
2	Forms of Security I	2	Assignment 2
3	Forms of Security II	2	Assignment 3
4	Forms of Security III	3	Assignment 4
5	Simulation in Security Planning and Management	4	Assignment 5
6	Meaning & Types of Security Threat I: Natural Threats	5	Assignment 6
7	Meaning & Types of Security Threat	6	Assignment 7

	II: Manmade Threats		
8	Information Warfare as a Security Threat	6	Assignment 8
9	Arms Production and Proliferation as a Potential Threat to Security	7	Assignment 9
10	War as a Security Threat	7	Assignment 10
11	Safety Measures to the Management of Natural Threats	8	Assignment 11
12	Safety Measures to the Management of Manmade Threats I	9	Assignment 12
13	Safety Measures to the Management of Manmade Threats II	10	Assignment 13
14	Civil Security: Meaning and Approaches I	11	Assignment 14
15	Civil Security: Meaning and Approaches II	11	Assignment 15
16	Meaning of Intelligence	12	Assignment 16
17	Intelligence Collection and Disciplines	13	Assignment 17
18	Intelligence Analysis and Evaluation	14	Assignment 18
19	Counter-Intelligence	15	Assignment 19
20	Data Mining and Automated Data Analysis	16	Assignment 20
21	Revision	17	
22	Examination	18	

Table 2: Course Overview

Presentation Schedule

The Presentation Schedule included in your course materials gives you the important dates for the completion of tutor-marked assignments and attending tutorials. Remember, you are required to submit all your assignments by the due date. You should guard against falling behind in your work.

How to Get the Best from this Course

In distance learning the study units replace the university lecturer. This is one of the great advantages of distance learning; you can read and work through specially designed study materials at your own pace, and at a time and place that suit you best. Think of it as reading the lecture instead of listening to a lecturer. In this same way that a lecturer might set some reading for you to do, the study units tell you when to read your set of books or other materials. Just as a lecturer might give you an in-class exercise, your study units provide exercises for you to do at appropriate points. Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit and how a particular unit is integrated with the other units and the course as a whole. Next is a set of learning objectives. These objectives shall let you know what you should do by the time you have completed the unit. You should use these objectives to guide your study. When you have finished the units you must go back and check whether you have achieved the objectives. If you make a habit of doing this, you will significantly improve your chances of passing the course. The main body of the unit guides you through the required reading from other sources.

Reading Section

Remember that your tutor’s job is to assist you. When you need help, don’t hesitate to call and ask your tutor to provide it.

1. Read this Course Guide thoroughly.

2. Organize a study schedule. Refer to the ‘Course overview’ for more details. Note the time you are expected to spend on each unit and how the assignments related to the units. Whatever method you choose to use, you should decide on and write in your own dates for working on each unit.

3. Once you have created your own study schedule, do everything you can to stick to it. The major reason why students fail is that they fall behind in their course work. If you run into difficulties with your schedule, please let your tutor know before it is too late to help.

4. Turn to Unit 1 and read the introduction and the objectives for the unit.

5. Assemble the study materials. Information about what you need for a unit is given in the ‘Overview’ at the beginning of each unit. You will almost always need both the study unit you are working on and one of your set books on your desk at the same time.

6. Work through the unit. The content of the unit itself has been arranged to provide a sequence for you to follow. As you work through the unit you will be instructed to read sections from your set books or other articles. Use the unit to guide your reading.

7. Review the objectives for each study unit to confirm that you have achieved them. If you feel unsure about any of the objectives, review the study material or consult your tutor.

8. When you are confident that you have achieved a unit’s objectives, you can then start on the next unit. Proceed unit by unit through the course and try to pace your study so that you can keep yourself on schedule.

9. When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment

is returned, pay particular attention to your tutor's comments, both on the Tutor-Marked
Assignment form and also on what is written on the assignment. Consult your tutor as soon as possible if you have any questions or problems.

10. After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unity) and the course objectives (listed in this Course Guide).

Facilitators/Tutors and Tutorials

There are between 8 and 12 hours of tutorials provided in support of this course. The dates, time and venue of these tutorials shall be communicated to you. The name and phone number of your tutor will be made known to you immediately you are allocated a tutorial group. Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulties you might encounter and provide assistance to you during the course. You must mail your tutor-marked assignments to your tutor well before the due date (at least two working days are required). They will be marked by your tutor and returned to you as soon as possible. Do not hesitate to contact your tutor by telephone, e-mail, or discussion board if you need help. You will definitely benefit a lot by doing that. Contact your tutor if:

- you do not understand any part of the study units or the assigned readings;
- you have difficulty with the self-tests or exercises; and
- you have a question or problem with an assignment, with your tutor's comments on an assignment or with the grading of an assignment.

You should make an effort to attend the tutorials. This is the only opportunity you have to enjoy face to face contact with your tutor and ask questions which are answered instantly. You can raise any problem encountered in the course of your study. To gain the maximum benefit from course tutorials, prepare a question list before attending them. You will learn a lot from participating by active discussion.

Summary

CSS 241 aims to expose you to the basic ideas and methodologies to security planning and management as well various issues and incidents that constitute threat to overall security arrangement of any people or society. As you complete this course, you should be able to answer the following questions:

- Explain the meaning of security and its approaches;
- Identify basic security ideas and policy actions;
- Clarify various forms of security as especially they constitute basic security management;
- Describe the application of simulation in security planning and management;
- Conceptualise the term security threat;

- Categorise security threats;
- Discuss various types of major natural security threats;
- Examine various manmade security threats;
- Draw inferences on how information warfare, arms production and proliferation as well as war constitute security threats;
- Propose safety measures to the management of both the natural and manmade threats to security;
- Explore how civil security can advance effective management of security in any community;
- Provide operational definition or meaning of the term intelligence;
- Elaborate on the activities and processes of intelligence of collection;
- Illustrate the processes of intelligence analysis; and
- Stress the importance of data mining and automated data analysis to intelligence gathering, intelligence analysis, crime investigation, crime prevention and detection, threat mitigation as well as security planning and management.

Finally, you are advised to read the course material appreciably well in order to prepare fully and not be caught unawares by the final examination questions. We sincerely wish you success in your academic career as you will find this course (CSS 241) very interesting. You should always avoid examination malpractices!

CSS241 BASIC SECURITY AND SECURITY THREATS

Course Developer/Writer	Monsuru Adegboyega Kasali Non-Violence and Intercultural Communication Advocacy Initiatives, Ibadan, Nigeria
Course Editor	Rasidi Okunola, Ph. D Department of Sociology University of Ibadan Oyo State
Course Coordinator	Adeniyi T. Adegoke, Ph.D Criminology and Security Studies School of Arts and Social Sciences National Open University of Nigeria
Programme Leader	Prof. Abdul-Rasheed Yesufu Dean, School of Arts and Social Sciences National Open University of Nigeria

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
No. 5 Dar es Salam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Published by

National Open University of Nigeria

Printed

ISBN:

CONTENT **PAGE**

MODULE 1

UNIT 1

SECURITY: MEANING AND APPROACHES

CONTENTS

1.0. INTRODUCTION

The word security emanated from the Greek word *Se-Cura*, meaning “to be in a state of no fear”. This state of being free from any threat within or without underscores the importance of putting in place actions and structures that can ensure the shelving of a people away from any harm. There is no doubt that security has been a subject that has attracted a rapidly growing interest and concern among the scholars in social sciences whereby a wide spectrum of issues on the subject – security has nevertheless been studied and new breakthroughs and findings have been made. The experience of the world in recent times emphasise a paradigm shift in security discourse. Traditionally, State is the custodian and ultimate beneficiary of the monopoly use of violence as advocated by Max Weber. Any internal or external threat challenging the authority of the State in monopolising violence was considered as a security threat.

During the Westphalia period, the major threat to the political sovereignty of any State usually emanated from another State. During that period, the threat to security usually involved state-to-state aggression, as there was little or no presence of intra-state violence. But, since the emergence of the Cold War in 1945, the main challenge against state has been internal threat to security where most countries became plagued with insurgency and civil wars as experienced on every continent. The end of the Cold

War in 1989 has widened the scope of security studies due to the emergence of states without any defined political boundaries.
This is evident in the enormous political sovereignty enjoyed by international terrorist networks that have created their own governments, standing army and other features of a modern state except defined geographical boundaries. The authority of these non-state actors is not limited by geographical boundary as their influence extends to several continents and they have become a major source of threat not only to national security but also to world security. The issue of security goes beyond the use of violence against any internal and external threats but also has included some other subjects like food, health, good governance, democracy, among others. We shall begin our task in this course by defining the term security and explaining various theoretical approaches to the study of security. I have the strong belief that you will find this unit very interesting.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Define the term security;

Identify various approaches to security; and

Discuss various approaches to security

3.0 MAIN BODY

3.1 **Definition of Security**

A layman definition of security is the protection of life and property of a person. The concept of security has undergone a transition from traditional conceptualization to a non-traditional meaning. Traditionally, security management was the unilateral function of the state especially if we consider the intellectual view(s) of some political theorists like Thomas Hobbes (1962) who argued that the essence of a state is to guarantee the security of lives and property and ensure law and order through its political sovereignty and monopoly of violence. This idea has made security issue a function of effective monopoly of violence, which the state applies to engender strict conformity and compliance to state laws by the peoples for effective security management.

But, in contemporary times, the definition of security goes beyond the traditional military ways of protecting the state against internal and external aggression. The fact is that since the end of the cold war, security management has assumed a new dimension. External threat to security resulting from international hostilities and aggression that characterized the cold war era has been replaced with non-traditional security threats like information warfare, drug trafficking, nuclear pollutions, disease epidemics like HIV-AIDS, corruption, human trafficking, (internal) insurgency, among others.

Nevertheless, this situation has led to multidimensional approach in security discourse and management. Now, many governments have realized that they can no longer monopolize the business of security in local domains as well as the world at large. This opinion has led to extending the security community to include private players (in security business), NGOs and above all, the civilians take the centre stage in security management. Like every other concept in social sciences, there is no universally accepted definition of the term security. Thus, scholars in the field of criminology and security studies have come up with different definitions of the concept of security according to their different theoretical rationalisations. At this juncture, let us look at some of the available definitions of the term security. Security can be defined as:

........an all-encompassing condition in which Individual citizens live in freedom, peace and Safety; participate fully in the process of governance; Enjoy the protection f fundamental rights; have Access to resources and the basic necessities of life; And inhabit an environment which is not detrimental To their health and wellbeing (South Africa White Paper on Defence, 1996).

......not only in terms of the internal security of the State, but also in terms of secure systems of Food health, money and trade (Tickner, 1994:180).

…….the degree of protection against danger, loss, and criminals (**Error! Hyperlink reference not valid.**).

......the protection of a person, property or organization from an attack. There are people who have distorted motivations to perform such attacks. The types of protection include prevention, response and pre-emptive attacks (://www.school-for-champions.com/security/whatis.htm).

......the protection of information assets through the use of technology, processes, and training (://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1244022 ,00.ht ml).

Despite the absence of consensus in the operational clarification of the term by different scholars, there is still a mutual agreement in the basic meaning of security among them, simply denoting the protection of lives and property. Meanwhile, the ways through which this basic objective can be actualised are the sources of the differences among the scholars. Notwithstanding, their different conceptual positions help us in broadening the frontiers of knowledge in security practice and management.

SELF ASSESSMENT EXERCISE

Define the term Security.

3.2 Approaches to Security Management

Managing security has remained an activity that requires the stakeholders to develop connections and relationships in theoretical terms, which assist policy-makers to explore a wide range of policy options, assessing their strengths and weaknesses in addressing the (complex) political, socio-economic and environmental threats to security. The basic approaches to security may include the following:

a) Idealism: This is a theoretical approach that emerged in the 1920s, as an initiative to guarantee world peace and security. This approach opines that security can best be managed through non-coercive or non-violent process, owing to the fact that violence would only give birth to further violence. The use of force or violence within national or international environment cannot guarantee any security.

   The members of this school hold that security can best be managed if government at all levels (from local to world) ensure that a security system 'based on development of civic culture on inter(national) agreements and treaties, stress on depolarization, demilitarization, transcendence of enemy imaging, and solidarity (Kasali, 2003: 43). This approach is also of the view that democratic governance as the ultimate mechanism for effective security management.

   Meanwhile, the emergence o World War II had undermined the relevance of this approach in the management of international security particularly as it concerned the issues of democratic order. The experience of the world population has not only shown that democracy cannot guarantee peace and security but some democracies can carryout offensives capable of jeopardizing national and international (security);

b) Realism: This is another traditional approach to security, which emerged as a response to the failure of the idealist approach in preventing the outbreak of World War II. The members of this school of thought agree that it is only through the use of coercion and deterrence that international security can be maintained. They also stress that apart from security, peace can only be engendered through judicious application of force or violence, which will generate effective dispute settlement and international security. This approach ensures management of security based on balance of power and multi-deterrence mechanisms. From the realist view point, states make decision in the attainment of their self – interest agenda, by evaluating available policy options and see how each of those options can fulfill or meet their security objectives.

   However, in the attempt to manage national security every country has begun to invest in the purchase of weapons to resist not only external security threats but also internal aggression. In this case, coercive power and military force play fundamental roles in the management of security. They will ensure compliance of state and non– state actors to the laws in the maintenance of world security. Also, in the management of internal security, state should ensure that its legitimate use of violence is reinforced by adequate military capability and mobility. This situation tends to lead to rapidly growing military expenditure. The amount of military hardware and personnel according to this approach, will determine how secure a nation will be. Realist model, therefore, led to arms race, in which states drastically increased their military expenditure in the defence of national sovereignty.

In developing countries, increased military budget has created internal tension and structural violence in which the local people have often lacked basic necessities, making them to survive marginally. On the African continent, this problem has attracted deepening political crisis, military coups and counter-coups, inter-ethnic violence, religious bestiality among others. The bottom–lime is that, rather than accumulating military wares for the protection of their various countries against the attacks from external forces, most governments in developing countries use the arms against their own citizens for a variety of reasons. Some of the reasons may include tenure elongation, racial discrimination, ethnic rivalry, religious chauvinism etc.

The violence experienced in Rwanda and Burundi made Africa a true reflection of Hobbesian state of nature. The madness that pervaded Hutus–Tutsi rivalry was monumental with high degree of bestiality. The violence was a nightmare! Nevertheless, foreign enemies can partner with local insurgents to undermine internal security of any nation as experience has shown since the end of World War II. The experience of the cold war era made great number of world states to align along the West–East polarity. Even, those countries that were not aligned (Non-Aligned Movement) were still mingling between the East and West blocs. Since the end of the cold war, the world has recorded more internal armed conflicts than international wars or aggressions, making it necessary to seek for another approach that can address the problem of increasing local insurgency in Africa and elsewhere;

c) <u>Pluralism:</u> Pluralist approach emerged in the 1960s. This approach was a departure from the state-centred security system that dominated the world system during the early cold war era. Pluralists articulated that balance of power, a key element of realism had not only failed to protect human race against insecurity but it had also aggravated pains that accompanied (such) insecurity.

The world began to experience a security dilemma resulting from the emergent danger posed by the politics of balance of terror where proliferation of weapons has become the order of the day. This approach explains why regional and world organizations have mandated their various agencies to carry out programmes that can influence international security policies, which may affect the self-interest of some (member) nations. This will bring us to the question of which national interest policies are internationally moral? Pluralists admonish states to discountenance any of their self interest policies that are considered to be immoral or capable of undermining international security;

d) Marxism: This approach became popular in security studies in the 1970s. According to this approach, economic factors and struggle for the control of state resources are the bases for security relations among states. Within the structure, the struggle for the control of means of production can lead to violent conflict situations between the proletariat and bourgeois.

Marxist approach contends that the state should control the economy and abolish private ownership of property and every individual should be catered for according to his/her needs. If the state unilaterally controls the economy, selfish pursuits, which form major security threat must be addressed. The issue of selfish accumulation of wealth would not arise if private ownership of property is discouraged. The crimes and threats that crop-up through the struggle for control of resources would have been eliminated, if no individual is allowed to own a property.

Nevertheless, struggle for the control of the state resources by individual actors tends to generate tension in the polity and those who perceive exclusion can resort to violence and other forms of criminality like armed robbery, terrorism, and insurgency. Weak nations or developing counties appear to be most palpable victims of such structural tension.

In the process, the insurgents engage government forces in armed struggle, and in replenishing their armoury, insurgents and government often use valuable resources (they are fighting over) in the purchase of weapons, most of which come from developed countries. In this case, powerful nations derive enormous economic benefits from such a situation of violence and insecurity in the weak states;

e) Social Constructivism: This is another approach of security, which emerged in the 1990s, immediately after the collapse of the Berlin Wall (the end of the Cold war). This approach advocates for more cultural understanding of security studies. In international relations as well as national politics, the self-interest of any nation is paramount, and it is considered as the driving force of its policy directions particularly as it relates to meeting its security goals.

State actors have now realized the need to pursue regional interest, even above their own national interests. This approach underscores the emerging interest nations are having towards collective security. This has created a new understanding in security relations among states. State actors have begun to show deep concern in the spill-over effect(s) of any insecurity in their neighbouring countries, on their own internal security. One of the reasons why Nigeria intervened and ensured the resolution of the armed conflicts in the region, i.e. Liberian and Sierra-Leonean crises, was the negative impact that those violent conflicts would have on her internal security.

The civil wars that plagued Sierra-Leone and Liberia generated large amount of refugees in the sub-region, and Nigeria was one of the host countries, that accommodated those refugees. Many of the refugees hosted by Nigeria were not properly disarmed. Some of them came in with arms, which found their way into the hands of some of local criminals, who used the weapons to further terrorize the nations. This situation has posed a great security threat to the nation.

Apart from the weapons exchanged for money, some of the refugees joined some local criminal gangs to engage in armed robbery and other violent crimes, constituting a threat to national security. The experience of the countries in the Great Lakes was horrendous as the region did not only generate the highest flow of refugees, but armed conflict also became an infectious disease that plagued a great number of counties in that region.

Moreover, in combating crime, several countries have formed international police (INTERPOL) community to arrest and prosecute or even repatriate criminal suspects who are creating security problems to any of the member nations. Few years ago, a notorious transborder bandit (Amani Tijani) who was the leader of an armed robbery gang specialising in carjacking, known to have robbed many innocent people of their cars in Nigeria. After robbing their victims, the bandits usually crossed to neighbouring Republic of Benin where the group resided. The cooperation between the police authorities in Nigeria and Benin paid off, leading to the arrest of the suspect(s) in Benin. The suspect was therefore repatriated to Nigeria where he is currently facing trial.

By and large, nations now appreciate taking regional approach in the management of their internal security. This is as a result of the (negative) impact that breakdown of order or insecurity in a country can have on its neighbouring countries. It is against this back-drop that countries sometimes sacrifice their national interests for regional interest. It is on record that the rising wave of crime and insurgency in Nigeria can be blamed largely on maladministration, but the upsurge of political strife in Liberia played a part in the security dilemma that Nigeria has since been experiencing; and

f) Human Security: There is no doubt that in the decade preceeding year 2000 witnessed a lot of contradictions and negativities in terms of war, which posed a great threat to national and international security. The spread of HIV-AIDS was rapid during this period with resultant case of pandemic. Global warming has emerged as a cankerworm ready to destroy the human race, and the volcanic nationalism that greeted post-cold war era has become a major source of state collapse. The subject of legitimate use of violence by the state has attracted a great debate, especially as we consider the unjustifiability in the exercise of power by some governments.

By the 1990s, the attention of the world population had shifted to redefining security and looking for the best approach that could guarantee effective security management, different from the traditional ones that had failed to address the increasing security threats. The search for the best approach led to the emergence of the term human security. This approach advocates for a paradigm shift. Rather than allowing the state to continue to define security, people who make up the state should be the ones to define their own security. Therefore, it is not the function of the state (or government) to determine security imperatives for the people but it is the people who should have the final say in deciding their own security.

So, the state traditional security measures of coercion and deterrence are moribund or outdated. Hence, policy-makers in several countries have adopted this approach as the guiding principle of their security laws. The consensus of state and non-state actors is now geared towards appreciating “any security issues, including without limitation, those of a political, strategic, economic, social, or ecological nature” (Vale, 1992: 100).

Nevertheless, the theoretical ingenuity brought about by the United Nations Development Program (UNDP) in its “Human Development” Report popularized the concept of ‘human security’ among the scholars and practitioners in the field of security studies and management (Henk, 2005: 2). We cannot but agree with the UNDP for reaffirming that:

The concept of security has for too long been interpreted narrowly: as security of territory from external aggression, or as protection of national interests in foreign policy or as global security from the threat of a nuclear holocaust. It has been related more to nation-state than people…..forgotten were the legitimate concerns of ordinary people….for many of them, security symbolized protection from the threat of disease, hunger, unemployment, crime, social conflict, political repression, and environmental hazards (UNDP Human Development Report, 1994: 22).

Since the 1990s, this approach has not only become the priciest bride among the state actors but also among several non-state actors including the Non Governmental Organizations (NGOs) that have acted spontaneously in the popularization of human security as an approach to security. One of the leading NGOs advocating for the global adoption of this approach is the Human Security Network. This organization has been championing the need to “energize political processes aimed at preventing or solving conflicts and promoting peace and development” (.humansecuritynetwork.org/network-e.php).

It is no news that several nations have articulated the relevance of human security approach in the formulation of their security policies. South Africa defined its national security in its "White Paper on Defence", which was published in 1996. As contained in the Paper:

In the new South Africa national security is no longer viewed as a predominantly military and police problem. It has broadened to incorporate political, economic, social, and environmental matters. At the heart of this new approach is a paramount concern with the security of people.

Security is an all-encompassing condition in which individual citizens live in freedom, peace, and safety; to participate fully in the process of governance; enjoy the protection of fundamental rights; have access to resources and the basic necessities of life; and inhabit an environment which it is not detrimental to their health and well-being (South African Department of Defence, 1996).

Similarly, Canada has also incorporated human security approach into its foreign policy formulation process(es). The country has redefined the concept of security from the traditional one to that which guarantees "safety for people from both violent and non-violent threats…..characterized by freedom from pervasive threats to people's rights, their safety, or even their lives" (Department of Foreign Affairs, Canada, 1999: 5). The country has also backed its new commitment with expending huge national resources in the promotion of human security worldwide especially in form of aids (see .humansecurity.gc.ca).

SELF ASSESSMENT EXERCISE

Discuss approaches to security.

4.0 CONCLUSION

Before the collapse of the Berlin Wall, scholars and practitioners in security had been confronted with the problem of identifying which of the available approaches was the best in the management of security nationally and internationally. Basically, various traditional approaches have focused exclusively on the security relations among state actors, relegating the relevance of individual people in security affairs. The traditional coercion and deterrence techniques are becoming moribund and ineffective in security management.

Non-state actors are becoming more visible in national and international theatres of violence, such that some individuals or groups have become more powerful than the state. A good example is Hezbollah (militant group) that is considered in several quarters as more powerful than the government of Lebanon. One of the reasons is that its (Hezbollah's) membership extends beyond Lebanon. Members of this militant group scatter across and beyond the whole Middle East. Al-Queda taught the whole world that commercial planes could be used as weapon of mass destruction in the 9/11 incident where thousands of people were massacred by crashing planes at the World Trade Centre and the Pentagon. There is need for world governments to adopt the new non-traditional approach, human security to address the structural security threats that bedevil most countries in the world.

The issues of hunger, poverty, proliferation of weapons, landmines, authoritarianism, environmental pollution and degradation, social injustice, political exclusion, crime, human rights abuse, illiteracy, economic deprivation, militarism, and maladministration, which human security seeks to solve, must be critically addressed in making security decisions. Thank God that several states have started adopting this approach. On the question of whether Nigeria will soon join the league of countries having human security as the foundation of their security agenda, it is only time that will tell. It is only time that will tell, if the country will move beyond its traditional AK-47 coercion and deterrence approach, which is state-centric. Human security approach is the most effective approach to security management. Apart from other reasons, it allows people to deliberate and decide their own security matters.

5.0 SUMMARY

In this unit, our focus has centred on describing the meaning of security especially through presentation of several definitions from different perspectives. Thereafter, we explained various approaches to security. Meanwhile, the first five approaches can be regarded as traditional approaches while the last approach is non-traditional, which advocates for paradigm shift in security practice and management. Therefore, human security advocates for ‘peopling’ of security in which the people define security matters rather than the state. The writer wishes to remind you that there are other non-traditional approaches, which could not be covered in this unit. You are hereby advised to search for other non-traditional approaches to security in the library or on the internet. Did you find this unit interesting? If yes, bravo! And in case you have any question regarding any aspect of this study, please contact your tutorial facilitator or other student(s) in your study group for assistance. Good luck.

6.0 TUTORED MARKED ASSIGNMENT

Write a short note on any five of the following approaches: Idealism, Realism, Marxism, Social Constructivism and Human Security.

7.0 REFERENCES AND FURTHER READING

Canada Department of Foreign Affairs and International Trade (1999). *Human Security: Safety for People in a Changing World*. Ottawa: Department of Foreign Affairs.

Henk, D. (2005). Human Security: Relevance and Implications. *Parameter* 35: 91-106.
Hobbes, T. (1962). *Leviathan*, New York: Collier.

Kasali, M. A. (2003). The Pacific Settlement of International Disputes in International Law: Origin and Dynamics of Diplomatic-Legal Manouverings to Bakassi Question. Unpublished M.Sc. Dissertation: University of Ibadan, Ibadan, Nigeria.

South African White Paper on Defence (1996). Pretoria: Department of Defence.

Tickner, J.A. (1995) Re-visioning Security. In: Booth, K. & Smiths, S. (eds.). *International Relations Theory Today*. Cambridge: Polity Press. 175-198.

UNDP, Human Development Report (1994). Also available on **Error! Hyperlink reference not valid.**. Retrieved on 10 January, 2008.

Vale, P. (1992). Can International Relations Survive? *International Affairs Bulletin* 16 (3): 98-119.

Error! Hyperlink reference not valid.. Retrieved on 2 August 2009.

://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1244022,00.html. Retrie- ved on 3 August, 2009.

.humansecurity.gc.ca. Retrieved on the 10th January, 2006.

.humansecuritynetwork.org/network-e.php. Retrieved on 10 January, 2006.

://www.school-for-champions.com/security/whatis.htm. Retrieved on 3 August, 2009.

UNIT 2

FORMS OF SECURITY I

CONTENTS

1.0. INTRODUCTION

Security is a subject that has attracted a rapidly growing interest and concern among scholars in the social sciences thereby generating a wide spectrum of issues on the subject. It has nevertheless been attracting new studies, which have brought-out new breakthroughs and findings in security approaches and methodologies. The importance of security cannot be over-emphasised, considering the amount of adverse effects that the absence of law and order can have on the overall development of any society or nation. The fact that emanates from this intellectual position is that security is very strategic to actualising any meaningful development and peace in any given community. In furtherance of our study of the meaning of security, we shall be discussing in the next three units, the various forms of security that exist. Meanwhile, we may not be able to cover all the existing forms but the basic ones will definitely be discussed.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Define the term computer security;

Explain various key concepts of computer security; and

Discuss approaches to computer security

3.0 MAIN BODY

3.1 Meaning of Computer Security

We are beginning our journey on the discourse-forms of security with the subject of computer security. Layman may define computer security as all aspects of security, which involves protecting our computing systems from malicious attacks and intrusion. Meanwhile, let us consider some other definitions of computer security.

Computer security touches draws from disciplines as ethics and risk analysis, and is concerned with topics such as computer crime; the prevention, detection, and remediation of attacks; and identity and anonymity in cyberspace (Kinkus, 2002).

Computer security is a branch of technology known as information security as applied to computers. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible.... (://en.wikipedia.org/wiki/Computer_security).

Computer Security can also be described as:

the concept of attaining a secure computing environment (ie, an ideal state free from risk or danger) by mitigating the vulnerabilities associated (**Error! Hyperlink reference not valid.**).

....a general term relating to measures designed to protect computer assets in all configurations (.securiguard.com/glossary.html)

Computer security can be described as an aspect of information security which basically involves putting some measures in place to secure your computers and networks, or simply protect them against infiltration, illegitimate access or corruption of data. In recent time, computers have replaced normal traditional paper system where information is stored in physical files. You go into government ministries, you often see files on the tables or shelves or storage cabinets marked with ‘confidential’. In Nigeria, almost every file is marked ‘confidential’ and the irony of it, is that any stranger can have access to any of these files because of the carefree attitude of many public servants, official corruption and absence of security consciousness that characterize the nation’s bureaucracy.

It is most disheartening the way important and valuable files get missing, with no trace of recovery. Several pensioners are losing their pension entitlements simply because their files cannot be traced. And such a situation may have security implication on the State. For instance, a pensioner who has a number of children in tertiary institutions, and is unable to have his entitlements because his file cannot be traced. If the retiree does not have any other means of survival, to take care of his family, the children will need to fend for themselves. And in the face of job drought, there is the tendency for (some of such) children to be tempted to engage in anti-social activities like ‘yahoo business’ (online scam), street begging, stealing, to mention a few, thereby constituting a threat to the security of the larger community.

Emotionally, the children of the deprived retiree will tend to develop hatred towards a system that denies their father of his entitlements. This problem may have also denied the poor retiree an opportunity to carry-out his financial obligations to the family. It is only when these children have creative thinking and positive perception that they might not develop negative emotions, which can sometimes lure them into social vices. I could remember a colleague of mine at the university who always complained of hunger and financial incapacitation due to late and irregular payment of the peanuts his father was receiving as pension. The abominable verification exercise, which pensioners are often subject to, appears to be a source of worry. Coming to the story of the retiree’s son, consequently, the guy had to fend for himself, and in the process due to his vulnerability, some of his peers in the neighbourhood introduced him into armed robbery. He was later arrested but many of his university colleagues were astonished and sympathetic too because he was not only homely but also academically brilliant.

The argument here is that if someone could engage in crime due to the inability of his father, to oblige him financially, resulting from late and irregular payment of his father’s pension by the government, then what would be the fate of a dependant whose father was not paid at all for the inability of the relevant authorities to trace the file that contains his employment records? The foregoing painted the danger inherent in ineffective storing and misadministration of information. There is no doubt that absence of proper management of information can provoke a security threat to any State.

However, through the use of computer, the long queue and frustration that adorn pensioners’ verification exercise would have fizzled out, and every genuine pensioner can collect his/her pension promptly and happily without stress. The traditional means of data management are becoming obsolete. The files that fill up a whole building can be saved in a small and compact storage device like computer hard disk or removable disks whereby one can store or/and retrieve or/and amend any file timely and easily. How much space do you think will be acquired, if we physically have to open files for ten million people? Here, it may involve occupying a very big building, which may cost several millions of Naira to acquire but with less than five hundred thousand Naira, we can get computers of high storage capacity that can accommodate several hundreds of millions of such files without taking any space beyond that where you mount your desk(s) that supports the computer(s). Even, one may not need a desk at all, with the use of computing systems like laptops.

If information is vital to the continued existence of any organization, it is pertinent to put in place necessary structures and applications to protect your computer(s) against any infiltration or damage. The emergent revolution in Information and

Communication Technology has rendered the traditional means of storing information like paper files moribund whereby computers have gradually replaced them. It is no surprise therefore, that the managements of many organizations in Nigeria have begun to mandate their staff to undergo various computer trainings in order for such to remain relevant in their various work places. Many public workers can now use computers effectively, as many government job functions are carried out electronically. Many state governments especially Lagos state have computerized their public service, as most services are now being rendered through electronic means. Taxes are currently paid by individuals and corporate bodies through electronic medium.

The Immigration Service in Nigeria has also gone computerized. Processing and issuance of passport is now done electronically, and this appears to be faster and more convenient. However, let us consider a scenario where the details of all those who applied for Nigerian passports in the last two years get erased through malicious attack from intruders or hackers. Another case is a situation whereby the data system of a commercial bank gets corrupted through virus attack. How do you think the bank will manage to get out of such crisis without any back-up? Considering these two scenarios, you may agree with me that it is important to provide adequate security for our computer system(s).

Essential measures and applications must be put in place to secure our computer system especially as security experts. The nature of the security profession demands for adequate computer security, and we should make enough efforts to protect our computer systems from malicious attack like corruption of data, theft, intrusion, illegal access to data, and damage emanating from natural disaster. In the subsequent part of this segment, we shall be discussing various ways to secure our computers but before we do that, let us quickly explain key concepts of computer security in order to stimulate a better appreciation of the subject.

SELF ASSESSMENT EXERCISE

Describe the term computer security.

3.1.1 **Key Concepts in Computer Security**

<u>Anti-Virus Software</u>: There is a conflict among scholars on the originator of anti-virus software but history has it that the first public virus removal task was performed by Bernt Fix in 1987 (Wells, 1996). Anti-virus software is used to detect, prevent and destroy any malware like computer viruses, worms as well as trojan horses. Apart from protecting the computer against malicious attacks, anti-virus also helps to detect spyware or any other programmes or websites that can constitute security threats to the computer system like virus attack, intrusion and hacking. It also assists the computer user to identify sites that are not secure, or those designed to perpetrate online scam, through prompt alert and warning of the imminent danger such sites pose to the user and/or system, and will advise that the user should not give the details of

his/her vital information or betterstill to close the suspected sites and avoid copying anything from such sites.

Anti-virus software is actually a set of computer programmes designed purposely to identify, block or destroy computer viruses and malicious agents with the aim of protecting the computer from information theft, corruption, hardware damage, to mention a few. There are various types of anti-virus software in the market today, including Norton, AVG, McAfee among others. Due to the way new viruses are generated almost on a daily basis for commercial, strategic or other reasons, it is very pertinent to upgrade the anti-virus software on one's computer from time to time, so that your computing system will be immune from any attack. Apart from virus attack, hackers may try to break into your system to steal, modify or delete some of the files in your system or the whole information contained therein.

Before the advent of the internet, computer viruses were usually spread through floppy disks (diskettes) but now computing systems get infected with viruses and other forms of malware through the internet. Before now, it was rare for computer to be infected with viruses through the use of recordable or rewritable discs but now the story is different. That is why it is advisable to restrict access of people into your computer and avoid the use of storage facilities like MP3, Flash disk, diskette etc, that have used somewhere else especially at commercial cyber centers without being scanned properly. It is also important to note that it is most appropriate to delete any virus infected files that cannot be repaired by the anti-virus package on your computer system.

Authentication: This involves a technique in which we create password to restrict access to one's computer. In this case, it is only those who can provide the correct password that can be allowed by the computer to gain entry into it. Authentication can also be defined as:

....the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual (**Error! Hyperlink reference not valid.**).

Sometimes, within the same system, there may be several users, each of whom will create his/her username and password before he/she can access his/her information on the system but the computer will prevent every user from gaining access to another user's information, if he/she fails to provide the correct username and password. There are several ways compute authentication is initiated by the system, and these may identify the users through username or/and password, identification cards, smart cards, as well as biometric systems.

Automated Theorem Proving: This is a verification tool in secure computing system that allows vital algorithms as well as code to be proven mathematically through which the specification of the computer can be met.

Backups: These are simple techniques that help us to secure information in our computing systems by copying and keeping our important files in another storage locations like a more secure section in the computer hard drive (less reliable because it goes with the computer in case of theft), MP3 storage device, i-pods, recordable and/or rewritable discs, tapes, flash disk, external hard drive and file hosting on the web.

It is noteworthy to know that there are inherent dangers in keeping files on the web, if adequate security cannot be guaranteed. Highly secure backups are supposed to be very safe and secure storage locations that are not easily susceptible to theft, loss, or destruction resulting from fire, heat, water, or even natural disasters. A good example is a university that has been existing for more than forty years, and experiences fire outbreak that destroys all its academic records. Without any backups, how do you think it will be able to supply the academic records of those who have graduated from the school? You answer may be the same as mine.

Capability and Access Control List: These techniques are usually used to guarantee privilege separation and compulsory access control.

Chain of Trust: This enables us to verify the authenticity of any software loaded on the system, through which we can identify the software certified authentic by the system's designer.

Cryptographic Techniques**:** These techniques are applied basically to reduce the risk of interception or modification of data whenever data are being exchanged between two or more systems. These techniques involve changing information in such a way that it will remain unreadable to any intruder when data is transmitted from one system to another. In this case, it is only the genuine recipient of the information that can unravel the content of the message while anybody who gains access to such message will not understand the content of the message unless it he/she can break the code to unscramble it, which may be very difficult if the encryption is done very securely.

Encryption: This tool is used to prevent any strange or unintended person from comprehending the content of a message. It involves scrambling of the information in a way that it will be unreadable by anybody other than the real recipient(s) whom the information is meant for. It is the recipient who has the code to unlock the information that can decipher a message. This approach can be used to send secret or very confidential information to several people irrespective of their number in as much they have the cryptographic key, which will enable them to decrypt it.

Decryption: Decryption can be defined as the tool used with the aim of "…reversing an encryption, i.e. the process which converts encrypted data into its original form" (://en.wikipedia.org/wiki/decryption).

Firewall: This technique helps to protect your system against any malicious attack or illegal access by hackers and intruders whenever you are online. It alerts you whenever it senses any intrusion, so that your computer will not be vulnerable to bugs.

Honey pots: These are computing systems made vulnerable to intrusion and attacks by hackers most times deliberately, to identify areas of defect or vulnerability to effect fixing it.

Mandatory Access Control (MAC): MAC is used to "protect the network and file systems, block users from accessing certain ports and sockets, and more" (://www.freebsd.org/doc/en/books/handbook/mac-understandlabel.html). It is however advisable for optimum use of policy modules, to load many security policy modules at the same time with the aim of providing a multi-layered security setting, and thus "….a multi-layered security environment, multiple policy modules are in effect to keep security in check" (*ibid*). The MAC application does not allow the users to change their access codes indiscriminately because all security features are usually controlled by the access rules presented by the selected security policy modules. Here, it is the system administrator that (absolutely) controls the MAC access rules.

Secure Cryptoprocessor: A **secure cryptoprocessor** can be said to be "a dedicated computer for carrying out cryptographic operations, embedded in a packaging with multiple physical security measures, which give it a degree of tamper resistance" (://neohumanism.org/s/se/secure_cryptoprocessor.html). The essence of a secure cryptoprocessor is to serve as the foundation of securing the system. It is a security sub-system that ensures protection of the system against any intrusion or malware. Some of the examples of secure cryptoprocessor include smart cards and ATM cards. The ways through which secure cryptoprocessor works include:

- *tamper-detecting and tamper-evident containment;*
- *automatic zeroization of secrets in the event of tampering;*
- *internal battery backup;*
- *chain of trust boot-loader which authenticates the operating system before loading it;*
- *chain of trust operating system which authenticates application software before loading it; and*
- *hardware-based capability registers, implementing a one-way privilege separation model* (://neohumanism.org/s/se/secure_cryptoprocessor.html).

Microkernels: Microkernel can be described as a computer kernel that enables relevant mechanisms, which help to initiate an operating system like low-level address space management, thread management, and inter-process communication. In a situation whereby multiple priviledge levels are offered by the hardware, "the microkernel is the only software executing at the most privileged level (generally referred to as supervisor or kernel mode). Actual operating system services, such as device drivers, protocol stacks, file systems and user interface code are contained in user space" (Joe, 1996 cited on ://en.wikipedia.org/wiki/Microkernel). In securing the computing system, microkernels are often used for systems designed for use in high security applications like KeyKOS, EROS and strategic security systems.

3.1.2 Approaches to Computer Security

a) Security Design: There are several ways through, which security systems are designed. It is paramount to mount effective security strategies that can ensure adequate safety for computing systems. One of such ways is to initiate the principle of least priviledge that "where an entity has only the priviledges that are needed for its functions" (://en.wikipedia.org/wiki/Computer_security). In this case, if an intruder gains access (illegally) into a part of the system, it will be difficult for him/her to access the whole system due to the fine-grained security.

It is therefore advisable to mount a security design that breaks the system into several smaller units with each of the units designed in a less complicated way, and may involve the application of automated theorem proving to verify the exactness of key software subsystems. In a situation where formal correctness is missing, careful application of code review and unit testing will be a best-effort approach in securing the modules. Enough efforts should also be made to discourage or eliminate security breaches by the system users, and it is therefore, important to create full audit trails that will assist us in detecting and determining the nature of breach, its degree and the time it occurs. Audit trials should be stored very discreetely in such a way that it will be difficult for the intruder to track it to cover up every trace of the illegal entry;

b) Security Architecture: Security Architecture is also a very viable approach to computer and information security. It simply means the design artifacts that explain the state of existing security controls or security countermeasures, showing how they relay with the general information technology architecture. The security controls basically focus on providing platform to enhance the capacity of the system to sustain quality attributes including confidentiality, integrity, availability, accountability and assurance (see **Error! Hyperlink reference not valid.**). Security Architecture assists us to identify the areas that demand much security measure, and thus, "if the plan describes a specific solution then, prior to building such a plan, one would make a risk analysis", but in a situation where "the plan describes a generic high level design (reference architecture) then the plan should be based on a threat analysis" (**Error! Hyperlink reference not valid.**); and

c) Secure Hardware**:** Computer security can be enhanced through hardware-based security because of the capacity of hardware-based security solutions to present strong resistance against bugs and intrusion. It can deny any intruder or hacker the avenue to read and write access to data.

SELF ASSESSMENT EXERCISE

What are the approaches of computer security?

4.0 CONCLUSION

The introduction of computer to the world population has really affected the culture of information generation, storage and amendment among people. People have now found it more convenient and safer to use computer to do all forms of activities regarding their collection, collation and storage as well as amendment of information. Computer systems, apart from being convenient, help us to store a lot of information and reduce the risk of data-loss through file-mishandling, file-missing and destruction of files by man-made and natural security threats or attacks. It is against the background of the importance of computer systems to information management that it is mandatory on our own part, to secure our computers and protect them against any malicious attack or hazard. In the subsequent units, we shall be exploring other forms of security.

5.0 SUMMARY

Due to the limited space and time we have on each of our lessons, in this unit, we were only able to discuss one of the forms of security-computer security. Notwithstanding, we began our discussion by examining the meaning of computer security. Thereafter, we explained various concepts of computer security, and the third and the last area of inquiry on the subject was a list of approaches to security management. As reiterated earlier, we shall continue our task of identifying and discussing various forms of security subsequently. Thank you very much for your patience and drive for learning.

6.0 TUTORED MARKED ASSINGMENT

a) What is computer security?

b) List any four concepts of computer security;

c) Discuss any two approaches of computer security.

7.0 REFERENCES AND FURTHER READING

Kinkus, J.F. (2002). Science and Technology Resources on the Internet: Computer Security. *Issues in Science and Technology Librarianship*, No. 36. Available on ://www.istl.org/02-fall/index.html. Retrieved on 30 August, 2009.

Wells, Joe (1996). *Virus Timeline*. Available on ://en.wikipedia.org/ wiki/ Microkernel. Retrieved on 31 July 2009.

://en.wikipedia.org/wiki/Computer_security. Retrieved on 1 August 2009.

://en.wikipedia.org/wiki/decryption. Retrieved on 2 August, 2009.

://neohumanism.org/s/se/secure_cryptoprocessor.html. Retrieved on 31 July 2009.

://www.freebsd.org/doc/en/books/handbook/mac-understandlabel.html. Retrieved on 31 July 2009.

://www.webopedia.com/TERM/a/authentication.html. Retrieved 1 August 2009.

.infosat.tamu.edu/students/glry/htmossa. Retrieved on 31 August, 2009.

.opensecurityarchitecture.com. Quoted on ://en.wikipedia.org/wiki/ Computer _ security. Retrieved on 31 July 2009.

.securiguard.com/glossary.html. Retrieved on 31 August, 2009.

UNIT 3

FORMS OF SECURITY II

CONTENTS

1.0 INTRODUCTION

In this unit, we shall continue our search of the basic existing forms of security. Do not forget, in the last unit, time and space only allowed us to discuss the meaning and key concepts of computer security (a form of security) as well as its various approaches. In furtherance of our study on forms of security, we shall be introducing a new set of forms of security to the reader. The two forms of security that we shall be considering in this unit for our study include information security and physical security. In that case, let us quickly browse through the various tasks we shall be undertaking in this study unit. These shall be found in the next segment of the unit.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Explain the meaning of information security;

Identify and discuss various approaches to information security; and

Define the concept of physical security; and

Describe key approaches to physical security.

3.0 MAIN BODY

3.1 Meaning of Information Security

Information security can be defined as a means of protecting information systems from any illegitimate access and use, theft, amendment, or malicious attacks or penetration. Information security can also be described as "the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations" (://www.ffiec.gov/ffiecinfobase /booklets/information_security/information_security.pdf).

Conceptually, it is important to clarify the differences in the meaning between the terms information security and computer security, which are often mistaken for each other. There is no doubt that the two concepts are inter-related because professionally speaking, they aim to advance the protection of information through the principles of confidentiality, integrity and availability. Despite the similar goals they both articulate or simply pursue, the two terms still have some differences. These differences are fundamentally found in their approaches, methodologies and variability in their areas of focus. Here, information security concentrates on ways to provide adequate confidentiality, integrity and availability of information but is less concerned with the data form be it electronic or print or any other forms of data. So, information security goes beyond the use of computer to create, modify, delete or store information. Therefore, its boundary goes beyond mere electronic medium.

On the other hand, in computer security, the central focus dwells on the techniques that enhance the availability and correct operation of a computer system with little attention on information stored and processed by the computer. One thing to note from the foregoing is the limited boundary that computer security acquires in information discourse. The point is that computer is entirely electronic, and there are other means like print through which we generate, amend, store or discard information. It is against this background that we conclude that information security is wider in scope than computer security, but each of them complements the functions and operations of the other.

Away from conceptual differences between information security and computer security, the experience of state and actors in the contemporary world has shown the growing relevance of information security. The increasing complexity of the modern state and sophisticated nature of contemporary business environment and corporations underscore the importance in mounting relevant mechanisms towards the protection of information and information system. For instance, let us look at the commercial banks in Nigeria in the 20th century, by the close of that century, virtually none of the banks could boast of having a capital base of US$ 1 billion. Again, during that period, online financial transactions like the use of ATMs, online shopping etc, were either non-existent or very limited.

Similarly, the period saw majority of the banks not having services that could enable their customers to save and withdraw their money from any of their branches without any geographic limitation, while most banks did not have up to one hundred thousand customers. But due to the opportunities provided by information technology revolution and recapitalization agenda of the Nigerian government, initiating the financial sector to be proactive in increasing their capital base and improving on their information system. The emergent information technology breakthrough especially the development of groundbreaking computer software and electronic machines like ATM have really helped in gradually fizzling-out long queues and the use of tally number as well as manual counting money by cashiers.

Nostalgically, I could remember those days when customers would wake up as early as 4am in order to reach their respective banks latest by 6am in order to be attended to early enough due to heavy traffic of customers. One could even reach the bank and meet some people already on the queue outside the bank premises. Then one would be asking himself if those met on the queue slept at home. But now, with the introduction of ATM, people can withdraw their money electronically anytime and anywhere.

Considering the opportunities provided by innovations in information technology, you may agree with me that financial transactions, trading, information exchange, mailing, communication etc, have been made so easy. You should however note that there are always two sides to a coin. Though, there is much convenience and fun derivable from modern information system but it can be awful considering the risk and danger one can fall into. For instance, if one wants to purchase items online and logs on a wrong web platform hosted to perpetrate scam, and you ignorantly provide your credit card details, and before you know, you have been duped. For this reason, people are being alerted to be very careful when doing online transactions.

One of the ways to reduce such risk is to install very strong security software that can easily detect and inform you if you are on a malicious site. Many organizations have gone into comatose or collapsed as a result of stealing, modifying, corrupting or deleting of vital information. It is therefore very important to put in place viable structures and programmes to protect your information. Now, let us quickly explain some of the methods we can use to safeguard our information systems and protect our information.

3.1.1 **Approaches to Information Security**

a) Confidentiality: In securing information systems, it is very germane to mount necessary machineries to advance the confidentiality of information. It is very paramount for the management of any organization to enlighten its staff on the need to take the issue of information very seriously. They need to know that it is very essential to prevent the organisation’s vital information from disclosure to unauthorized person(s) or system(s). Stiff penalty should be applied against any erring staff to deter others from doing the same. By commission or omission, if confidential information gets into the wrong hands of unauthorized person(s) or system(s), it will amount to a breach of confidentiality.

In procuring an international passport, you can log-on the website of the Nigerian Immigration Service to begin the process for your e-passport application. After filling the necessary forms online, you are requested to proceed with your payment, and here, you are given two options: offline or online payment. You may decide to do the payment online with use of your ATM card. In the process, the system will demand for your ATM details through ETRANSACT platform, and you provide it correctly. The gateway will debit your account where the ATM card domiciles, and consequently you will be allowed into the next stage of the application process after the confirmation of your payment, which will be electronically receipted.

Here, you need to be careful by not allowing anybody to peep into your financial transaction to avoid an unauthorized person to have access to your secret (pin) code, and if you allow such to happen before, during or after the period of transaction, you have committed a breach of confidentiality. You should know that it is incumbent on the organization(s) you transact with online to uphold the principle of confidentiality. Expectedly, when you are making your transaction, your credit card or ATM card details including pin-code will be transmitted from you to the organization/party with which you transact, and the details will also be transmitted from the said organization to a transaction processing network.

The system will ensure that confidentiality is enforced by encrypting (refer to 3.1.1 of last unit for the meaning of encryption) your ATM details especially the pin-code during the transmission, which are stored in a very secure location with highly restricted access. In a situation whereby you confirm that unauthorized person(s) has access into your financial details while the fault or criminal intent does not emanate from you, you have the right to institute a legal action against such erring organization for a breach of confidentiality.

Even if your spouse is allowed to access your bank statement account without authorisation is a breach of confidentiality, and the affected person can institute a legal action or warning to the bank management for the breach, or may close down his/her account for lack of security necessitated by the confidentiality breach. If one has the right to sue for a breach of confidentiality that involves his/her own spouse let alone a stranger or a distanced person, it is evident that information security is very important. It will be baseless, if the management of an organization argues that it will not be liable if an offence of breach of confidentiality is committed by any of its staff without its involvement against any customer especially if it involves loss of money.

Recently, due to importance of information, the approach of **due care and due diligence** has been adapted in information security. **Due care** involves measures and actions that are taken by a company not only to protect its corporate image but also show liability for all activities that take place within it, and establish regulations that will help to protect the company, its resources and employees. **Due diligence** means "continual activities that make sure the protection mechanisms are continually maintained and operational" (Harris, 2003). Therefore, if an organization fails in its responsibilities to check the activities of its staff, it will definitely be liable for any misdeed perpetrated by any of its staff such as disclosure of a customer's information to an unauthorized person, leading to a breach of confidentiality;

b) Integrity: Integrity can be described as a way of protecting information by restricting access to modification of data without authorization. Here, no amendment can be made on the data without authorization. In information security, efforts should be made to restrict activities of users of the systems from any data modification without being authorized. There are several ways through which the integrity of an information system can be violated. One of such ways is accidental or deliberate exposing of the system to malicious attacks.

Undoubtedly, this kind of violation occurs in many organizations where employees exhibit nonchallant attitude or criminal intent to compromise the integrity of the system. For instance, in some organizations with large network of information systems, family members, siblings or friends and even neighbours visit some employees, and many of these visitors may be allowed to use the organization's computers especially where they are connected to the internet. These use all sorts of storage facilities to download information from the internet. This attitude is likely to violate the integrity of the information system because apart from exposing the system to malware or virus attack, it will also allow strangers or visitors to have access to information, which ordinarily they are not supposed to;

c) Availability: Information system cannot be complete if there is no availability of information. It is the availability of information that makes information system what it is. Therefore, it is imperative to have a network of actions functioning well. These actions include the computer system that is tasked with the storing and processing of the information while the security controls do the protection of the system, and the communication channels enable the users to access that information.

If we consider this network of functions, we may agree that it is difficult to have 'high availability systems' in countries like Nigeria where there is frequent power outage that can easily disrupt the operation of the system. High availability systems are those systems that are always available, and demand necessary mechanisms to be brought to bear in order to prevent disruptions that may result from hardware failures, power outages, physical destruction of the information systems, to mention a few;

d) Authenticity: Information security demands that we can just collect information whether electronic or print for the sake of it, but we should endeavour to clarify the authenticity or genuineness of such information. It is by so doing we can have reliable and quality information;

e) Risk Management: Everything about life is a risk. There is risk, even in the relationship between two or more people. How do we describe risk management? According to CISA Review Manual (2006), risk management can be described as:

…..the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.

Risk is the everyday business of each man. Sometimes, we decide out of the blues to see a loved one in his/her place work, even after calling him/her of our coming, the subconscious still has a doubt about meeting him/her at the office because every second is clouded with eventuality. It is possible for the receptionist to inform us that he/she had an emergency from the headquarters and he/she tried to get you on phone to inform you about the new development (urgent call to report at the headquarters) but he/she could not reach on phone.

Considering the above scenario, you may agree with me that risk is second nature to man. The decision of a man and a lady to get married is a risk: the marriage may succeed or fail. It is against this background that many people adopt various approaches or measures to manage risk in their relationships. In information security, risk management is very essential because it determines the preparedness of an organization against any threat as it relates its information system.

Furthermore, in as much that information from its collection, modification to erasure involves risk, it is pertinent to develop countermeasures or controls to manage the risks but it is more important to “strike a balance between productivity, cost, effectiveness of the countermeasures, and the value of the informational asset being protected” (**Error! Hyperlink reference not valid.**), meaning that it is not appropriate to spend too much money or employing highly productive and effective in securing an information asset that has little importance to the overall interest of an organisation; and

f) Information Classification: There are different types of information in information system, and there is the need to classify these according to their level of importance and confidentiality. By doing so, we will be able identify the amount of protection to be accorded to each of these available information. For the purpose of engendering culture of information security, it is imperative for an organization to adopt a classification policy, so that it will be able to determine the required security controls of every information in accordance with its classification.

For instance, the head of an organization is having an extra-marital affair with a former female staff who he communicates on regular basis. May be because he is not internet-literate and always asks his male secretary to help him send mails to his 'lady-friend' while mandating the secretary to classify the mails as **top secret**, giving more importance to such mails than the very important information of the organization. This reflects a clear case of misuse of office and misclassification because it abnormal to place private issues above those that concern the organization and the work environment.

Within an organizational setting, we can classify information based on the value of it to the organization. In private organizations, classification models are usually labelled as: **public**, **sensitive**, **private**, **confidential**. But in big security outfits and government organizations the classification labels used include: **unclassified**, **sensitive**, **but unclassified**, **restricted**, **confidential**, **secret**, **top secret.** These classification labels are listed according to the security controls needed in protecting them, and the classification exercise should be continually reviewed.

SELF ASSESSMENT EXERCISE

Explain approaches to information security.

3.2 Meaning of Physical Security

Physical security involves creating designs that deter malicious entry into a facility. Here, the facility can be described within various contexts. It may mean office or private apartment, information systems, safe, among others. Physical Security can also be described as:

...the measures used to provide physical protection of resources against deliberate and accidental threats (.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html)

......protecting the system unit, system devices, and backup media from accidental or deliberate damage (http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzamv/rzamvbasicterm.html).

......the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism (://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1150976,00.html).

Due to revolution in modern technology, many innovations have been made in fortifying the security of facility. For instance, there are some computers that will demand for your biometric information before you are granted access into it. When we are talking about biometrics, we are not actually talking about username and/or password. The security technology of biometric usually involves hi-tech security measures especially where the computer will request to take the finger-print and eye(s) sample of the intending user to know his/her permission status. If the specimen is not found to be among the list of authorised users, you will not be able to gain access. Some of these systems are made in a way that if you make any attempt to forcefully gain (illegal) access, the machines will alert the relevant security guards of the intrusion attempt, and before you know what is happening, the security guards are there to effect your arrest.

I know many of us may be wondering why Automated Teller Machines (ATMs) are not usually attacked to get the money loaded in them. The truth is that most times, especially in developed countries, attempting to steal money in the ATMs is usually an effort in futility because, even, one is able to gain entry into the machine, the money will be destroyed. The machine may destroy the money by making some stamps on it, so that such money can be identified as stolen money from the ATMs. And in this case, nobody will accept the money and the law enforcement agents will also be alerted to arrest the culprit.

Meanwhile, I don't think we have orientation to that extent in Nigeria, which will make the people to identify money stolen from ATMs. Please, be cautious not to mistake breaking into ATMs to steal money loaded in it or engage in illegal ATM transactions like the theft of someone's ATM card. Here, we are discussing a situation where someone destroys the automated teller machines to steal the money loaded in it. Notwithstanding, in Nigeria, the security measure to deter criminals from looting the money ATMs may be by automating the machines, if they suspect such illegal entry, to destroy the money in it, so that they can become unspendable for the looters.

SELF ASSESSMENT EXERCISE

How do you describe physical security?

3.2.1 **Approaches to Physical Security**

Summarily, physical security can be explained from three different approaches, all of which are interdependent in order to provide adequate physical security for any facility. These approaches include the following:

(a) The first approach is concerned with mounting of obstacles or barriers that can prevent potential attackers, intruders or malicious personalities from gaining easy access into facility. The threats being accidents, environmental disaster or human attackers will be impeded by putting in place some measures like multiple locks, fencing, walls, and fireproof safes, to mention a few;

(b) The second perspective to physical security is the installation of surveillance and notification, which will help us to optimise the security of the facility by monitoring and detecting the activities of (potential) attackers to the facility. This involves the use of such security methods like installation of lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras; and

(c) The third approach involves putting in place measures that can help in effecting the arrest of attackers or hazards. For instance, there should be security guards that will act promptly and effectively when alert of attack is raised to arrest the attackers. Also, in fighting fire incidents, it is expected for us to have fire-fighting equipment or call professional fire-fighters to come to the rescue to quench the fire. There is the need too, to have in place emergency workers and disaster managers for hazard and disaster mitigation. These and other measures will help us recover quickly from accidents, fires, or natural disasters.

SELF ASSESSMENT EXERCISE

Explain the three basic approaches to physical security.

4.0 CONCLUSION

Considering the various forms already discussed within the last two units, you will agree with me that the security profession is very versatile. This is because each of these forms demands expertise in the fields. And that is the reason why we have different departments, divisions or areas in security sector. In this case, it is expected to place security employees into various available departments according their expertise in the relevant fields. It is only when this is done that there can be optimal performance among the security professionals. In the next unit, we shall complete our task in explaining various forms of security.

5.0 SUMMARY

In this unit, we continued our discussion on various forms of security. The first form of security we discussed was information security. Consequently, we explained the meaning of information security, as its various approaches were also explained. Thereafter, we highlighted the second form of security in this unit, as we described what physical security is all about. Our final area of discourse, however, was plotting an inquiry into the list of approaches to physical security. At this point, it is my belief that you have found this unit intellectually stimulating.

6.0 TUTORED MARKED ASSIGNMENT

Write a short note on:

a) The Meaning of information security and any three of its approaches; and

b) The meaning of physical security.

7.0 REFERENCES AND FURTHER READING

CISA Review Manual (2006). *Information Systems Audit and Control Association*

://en.wikipedia.org/wiki/Information_security. Retrieved on 1 August, 2009.

://searchsecurity.techtarget.com/ sDefinition/0,,sid14_gci1150976,00.html. Retrieved on 2 August, 2009.

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzamv/rzamvbasicterm.htm. Retrieved on 30 August, 2009.

://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf. Retrieve on 2 August 2009.

.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html). Retrieved on 30 August, 2009.

UNIT 4

FORMS OF SECURITY III

CONTENTS

1.0 INTRODUCTION

In the two previous units, we have discussed some of the basic forms of security including computer security, information security and physical security. To complete our task, we shall be explaining some other forms of security in this unit, which will include infrastructure security, seaport security, airport security, food security, and a host of other forms of security. Before we go into the nitty-gritty of these, let us quickly look at the objectives of this study.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Describe the meaning of infrastructure security;

Discuss what seaport security is all about;

Elucidate on the meaning of airport security;

Explain food security;

Define health security;

Clarify the meaning of economic security;

Examine what environmental security denotes.

3.0 MAIN BODY

3.1 Infrastructure Security

Infrastructure security can be described as that aspect of security designed purposely to provide protection for specific infrastructure particularly those infrastructure considered critical. The examples of critical infrastructure may include airports, sea ports, railway, network communications, hospitals, the Central Bank, dams, and oil refineries among others. Highways and bridges are also an aspect of critical infrastructure (://www.tsa.gov/travelers/highway/index.htm). Due to the importance of these infrastructures on the lives and overall wellbeing of the people, it is paramount to provide adequate security for them and immune them against any threat or attack.

Take for instance, if the dams or water systems that supply water to all households in a community are poisoned, you can imagine how many lives will be lost due to that attack. So, every government is expected to make efforts to equip infrastructure considered critical with enough security in order to avoid disaster. Another example is where the airport is not well secured and there is no doubt that there is tendency for it to be easily attacked by terrorists or saboteurs. If an airport or seaport is considered porous, it will be easy for enemies to bring into the country harmful and destructive materials that can undermine the security of that country.

Nonetheless, this shows how important it is to provide adequate security for infrastructure. It is a matter of fact that any damage intentionally or accidentally done to critical infrastructure will have far-reaching effect on the economy and overall security of a country. For instance, the continued destruction of gas pipes often disrupts level of power supply in the country with serious consequences on the power generation capacity of the Power Holden Company of Nigeria (PHCN). Threats which can damage infrastructure basically include the following (which shall be discussed extensively later in this course):

- Sabotage;
- Terrorism;
- Natural disaster; and
- Information warfare

SELF ASSESSMENT EXERCISE

What is infrastructure security?

3.2 Seaport Security

Ports are simply passages that lead into any country. Apart from seaports, people also use airports for the shipment of their cargos from one destination to the other. Meanwhile, the quantity of loads will determine which of these two ports should be used for the shipment. The seaports are where major shipping activities take place. And they are also vulnerable to security threats. for instance, through seaports, some (unsuspected) criminals can bring in hazardous goods like expired drugs, contraband products, illegal arms and ammunitions, among others. At this point, how do you describe seaport security? Seaport security can simply be described as:

...the defense, law and treaty enforcement, and counterterrorism activities that fall within the port and maritime domain. It includes the protection of the seaports themselves, the protection and inspection of the cargo moving through the ports, and maritime security (://en.wikipedia.org/wiki/Port_security).

There is no doubt that seaport security is very strategic to the political sovereignty and security of any country, and that is why governments of various countries take the issue of fortifying their ports as a very important one. The reason is that any government that fail to secure its seaports can be said to be on the verge of losing its sovereign power because not only the government but also the public at large that will be vulnerable to threats especially if enemies bring harmful and destructive materials into the country.

For instance, if there is no provision of sufficient security at the seaports, there may a situation of proliferation of weapons and small arms in that country, and terrorists can easily take over the ports. Destructive weapons like bombs, guns, or chemical weapons among others can be hidden and later used against the country. This view is shared by Greenberg *et al.*, contending that:

...whenever and wherever a container is handled during movement represents a potential vulnerability for the security and integrity of the cargo (Greenberg *et al.*, 2006 cited on ://en.wikipedia.Org/wiki/port_security).

There is no doubt that poor security handling of cargo can expose the country to security risk. In a country where there are sharp ethno-religious divisions like Nigeria, circulation of weapons can engineer insurgency and growing criminality as being experienced in the country in recent times. The level of sophistication in armed robbery operation compared with the weapons that bandits use in recent times, calls for total overhauling of our security sector and policy. It is a fact that most of these dangerous weapons are not manufactured locally but come into the country through the seaports and borders. The attendant consequences that accompany arms proliferation in Nigeria underscore the strategic relevance of effective port security.

SELF ASSESSMENT EXERCISE

Describe seaport security.

3.3 Airport Security

An airport is a place that involves an aspect of transportation. People travel either by road, sea or rail or air. All these means of transportation deserve to be provided with sufficient security. It is no exaggeration that the airport has continued to receive greater attention due to very strategic reasons. One of the reasons is that apart from being the most popular means of transportation, it is the fastest. It is a means of moving people from one destination to another, as well as for transporting goods. The journey that may take a ship three weeks or more can be covered by a plane in hours.
Airport accommodates a large number of people including the travellers, the crew and management of various airliners present at the airport(s) as well those who escort travellers to departure and those waiting to receive travellers on arrival. It is a network of people having different motives and it is important to put in place adequate security to protect lives and property at the airport.

The airport is also sensitive that it has become one of the veritable avenues being exploited by terrorists to carry out their attacks. The ugly incidents of terrorist attacks in many airports have necessitated the need by various countries to fortify security in their airports with the aim of making their airports less vulnerable to enemy's attack. Previously, less attention was paid to screening passengers for possession of arms and weapons which were usually hidden in their hand bags Some of the incidents may include arbitrary killing of innocent civilians by terrorists and disgruntled elements.

A good example of terrorist attacks is that of a Cubana Flight 455 from Barbados to Jamaica hijacked by terrorists on October 6, 1976 in which seventy-three people were murdered. On 30th May, 1972, a gang of three terrorists who were linked to the Japanese Red Army, shot and sporadically threw grenades at people at Lod Airport (now Ben Gurion International Airport) in Tel Aviv, Israel. Before they were overpowered, they had already killed twenty-four people and no less than seventy-eight people sustained various degrees of injury.

Also, in December 1985, the Rome and Vienna airports became targets of terrorist attacks. The terrorists took advantage of security lapses in these airports to carry out their nefarious acts. They shot and threw grenades at people and this led to the killing of no less than 20 people. The worst of all was the September 11, 2001 terrorist attack where some commercial planes were hijacked by terrorists linked to the Al-Qaeda network and deliberately crashed into the World Trade Centre and Pentagon while one meant to be crashed on the White House but was forced down by the passengers on board, missing the target.

3.31 Elements of Airport Security

Due to the large number of people being accommodated on a daily basis at the airports worldwide, various governments have begun to install different security systems. The infrastructure in most airports, especially in the US and UK since the 9/11 incident are being fortified with all sorts of security gadgets and procedures, as dictated by kinds of security challenges being experienced in various airports. For example, before now, the presence of touts and area boys was very evident in major airports in Nigeria. During that time, stealing of travellers' belongings and baggage was very rampant. The new security measures put in place since the civilian administration of Obasanjo (1999-2007) has drastically reduced the presence of touts in our airports. The incidence of missing baggage is reducing fast by the day. Let us quickly discuss some of the elements of effective airport security.

(a) Airport security personnel: The enforcement authority in the airports very according to the class of each airport. There are first class airports that can serve as international airport to be used as entry and exit point for travellers coming into or leaving the country. Conventionally, an international airport must definitely fulfil international aviation safety standards and should be equipped with facilities that can accommodate big aircrafts. The reason is that not all aircrafts can be accommodated by every airport. That is why some airports are used for local travels, many of which can only accommodate relatively small aircrafts.

Apart from the class of airports, the amount of security threats being experienced by an airport also determines the level of security to be provided in the place. By and large, most incidents of terrorist attack are usually effected through international airports, and this makes it pertinent to assign adequate security personnel there. Unlike countries like the United States where state and local governments have the highest control in the provision of security personnel to the airports, in Nigeria, airport law enforcement whether in local or international airports is largely controlled by Federal law enforcement agencies. The type of security personnel arrangement, you are likely to find at any international airport depends largely on the security policy of that country. For instance in Nigeria, there is absence of state police and no state government can provide security for any local airport without seeking assistance from the Federal government. Generally, the security agencies that can be found in airports may include:

- Policemen and officers specially attached to the airports;

- A permanent police station equipped with adequate equipment and competent personnel;

- Members of the Public Intelligence Community like State Security Service (as in Nigeria) who will be stationed at strategic locations within and outside the airports to gather security-related information that can be used to prevent or reduce crime or terrorist threat at the airports;

- Some members of (other) paramilitary agencies like Immigration Service and Customs Service to identify illegal immigrants, importers/exporters of harmful and banned products, and other culprits which should be arrested, investigated and if found wanting, they should be subjected to immediate prosecution;

- Emergency team that can respond timely and effectively to events of disaster like plane crash or fire outbreak at the airports;

- Anti-bomb experts to detect concealed bomb items or detonate any explosive found at or around the airports;

- Trained police dogs should also be used for the detection of explosives, hard-drugs and dangerous objects;

- Location of military barracks or situating a unit consisting of the military forces within the airports to provide complementary security services at the airports in protecting the nation's airports against any internal or external aggression;

- The use of Private Guards: Private security personnel can play complementary roles in providing security to the airport(s). For instance in Spain, private security officials are allowed by the government to provide security services at the airport. The airliners can also be encouraged to contract private security guards, the practice which exists in some countries. Some of these guards if not able to conduct the main screening at the screening points, can still use the method of "screening the passengers by observation techniques" (SPOT) that is already being used in several airports in the United States (://en.wikipedia.org/wiki/Airport_security); and

(b) Installation of security equipment: In recent times especially resulting from the experience of the September 11 terrorist attack in the US, most countries have fortified their airports with sophisticated security equipment. With metal detector, security officials can easily identify someone with arms or weapons like knives and other sharp objects that can be used to harm passengers and crew on any aircraft. In most international airport, it is illegal for restaurant operators within specific locations in the airports to use plates that may be converted into weapons by terrorists. In those restaurants, the operator use plastic to serve their customers. Technological advancement has brought about invention of very effective explosive machines or gadgets like X-ray machines, explosive trace detection (ETD), and puffer machines.

These machines are used to conduct screening for baggage and other travelling loads with the aim of detecting if there are explosive substances particularly volatile compounds that can make explosives using gas chromatography. According to Edward J. Staples (Ultrahigh-speed) gas chromatography (GC) can be described as:

....a powerful method for analyzing odours, fragrances, and chemical vapours produced by explosives, chemical and biological weapons, contraband, and hazardous industrial materials. A new chemical-profiling system directly measures odour concentration and intensity with an integrated GC sensor. Using a solid-state surface- acoustic-wave (SAW) sensor with electronically variable sensitivity, it identifies the chemical species in the vapours inside cargo containers and determines their concentrations in 10 s with picogram sensitivity (://www.aip.org/tip /INPHFA/vol-10/iss-3/p22.html).

The invention of backscatter X-ray scanners makes it possible to detect any hidden weapons on a any passenger. Here, passengers are asked to move close to a flat panel and in the process a high resolution image is produced through which someone with weapon(s) can be identified and arrested immediately for further interrogation.

SELF ASSESSMENT EXERCISE

What is Airport security?

3.4 **Food security**

The situation brought about by the introduction of exclusively crude oil economy in Nigeria in the 1970s has put the agricultural sector of the nation's economy into comatose. Nigeria which used to be one of the major food baskets and exporter of agricultural products in the world has become a perpetual importer of food items, meaning that, adequately feeding the masses is becoming a difficult task. There is no doubt that the agricultural sector has however become moribund. More than 70% of urban dwellers go about on empty stomachs. Hunger has continued to make people become more vulnerable by the day. This situation has been one of the major contributing factors to the increasing crime rate in the country especially the urban centres. In order to make food available abundantly to the people, government needs to adopt strategic and policy actions that can engender food security in the country. Then, what is food security? Food security can be described as:

...the reliable availability of a sufficient quantity and quality of nutritious food for a population (.personal.umich.edu/~alandear/glossary/f.html).

.. the availability of food - in other words whether it is physically available and if so at what price. The term is sometimes confused with that of food safety which refers to the

extent to which food is safe to eat (http://ec.europa.eu/agriculture/glossary/index _en .htmm).

...having access at all times to enough food for an active, healthy life (.pbs.org/ wgbh/rxforsurvival/glossary.html.

Bearing in mind the foregoing definitions of food security, you may agree with me that availability of food is very germane to the maintenance of law and order in any society. It is therefore important for every society or country to initiate policies, which can create opportunities to providing the people with food in qualitative and quantitative terms. Although, food security underscores the strategic importance that self sustenance in food production has on the security of any nation. The interdependence that dominates relations among nations also includes food. This is because there are particular types of agricultural items that cannot be grown in one country but which can be found in another country. For the fact that food is not luxury but necessity, a secure society will always undertake activities that will enhance their capacity to produce food locally, and endeavour as much as it can, to avoid importing the food items it can produce locally.

SELF ASSESSMENT EXERCISE

How do you explain the meaning of food security?

3.5 Health Security

This involves safety against pandemics and diseases. It is part of government responsibilities to provide health security for its citizens, knowing the impact that good health condition(s) can have on the development of any country. That is why in advanced countries, government provides platform to promote healthy living among the people. Health security is very crucial to national development, and that is the reason why countries like the United States have created opportunity for their people to access national health insurance scheme, where everybody will make contribution (premium) to the scheme. When people fall sick, there is insurance cover that will take care of their hospital bills according to their policy type(s).

In addition, most governments usually have some strategic interventions to respond to health crisis and pandemics. One of such interventionist techniques is awareness programme educating people about the danger of the outbreak of some diseases particularly those that are infectious like HIV/AIDS, SARS, and tuberculosis, to mention a few. Enlightenment also helps to guide people against (reckless) lifestyles and ignorance, which can aid spread of disease(s) especially those with high contagion.

Also, in most states sanitation officers are appointed by government to ensure strict compliance of the people to environmental and sanitation laws. The reason is not only to ensure good sanitation behaviour but also to guarantee the health security of the state. Another way of providing health security is by putting in place free health services for the people. Though, this kind of programme is very expensive, some governments still take up the responsibility of providing both qualitative and quantitative health services to the people at low cost. The purpose of doing this is to provide health security for the people.

SELF ASSESSMENT EXERCISE

Define health security.

3.6 Economic Security

This can be described as a way of putting in place measures and strategies that will ensure that every individual in the state is not only entitled to employment but also has the right to a living wage. In advanced countries, government often puts in place social security for citizens who are out of job whereby stipends are provided for the citizens to keep body and soul together. But, it is quite unfortunate that in most developing countries, unemployed people are left to their own fate, such that nothing is provided by government to ameliorate the plights of unemployed citizens. The people who have jobs don't have job security as several employees are cheated and underpaid by their employers.

This situation has therefore been one of the major factors responsible for the increasing criminality and criminal activities among the people especially the youths. It is important to know that economic exploitation, which is an aspect of economic insecurity cuts across all spheres of our national life. It is one of the factors responsible for poor quality of personnel in Nigeria Police making it inept as a security institution in discharging its primary functions (see Alemika, 1997).

SELF ASSESSMENT EXERCISE

How do you define economic security?

3.7 Environment Security

The concept of environment has begun to dominate international discourse. The issue of environmental pollution has continued to attract the attention of the individuals, Non-Governmental organizations (NGOs), nations as well as international organizations. It is imperative, that we consider the adverse effects of environmental hazards on the people, so that government and the people can ensure the security of their environment. Conceptually, environmental security can be described as:

....ability of a nation or a society to withstand environmental asset scarcity, environmental risks or adverse changes, or environment-related tensions or conflicts (://www.pacinst.org/reports/environment_and_security/env_security_and_climate_change.pdf).

.....the total surrounding or external conditions within which an organism or a community exists (Adeboyejo, 1994: 74).

Within the world body (the United Nations), efforts are being made through the (relevant) agency – the United Nations Environment Program (UNEP), to monitor environmental issues, and make reports and plans for such issues and to act and promote legal instruments on environment. If we want to talk about environmental security, our focus should be on the atmosphere, lithosphere hydrosphere and biosphere. People now talk about issues like damage in the ozone layer, climate change, water pollution and environmental degradation (to mention a few). Environment has great impact on the general well-being of the people, and that is the reason why increasing interest of state and non-state actors on environmental protection and security has become evident. The growing interest since 1980s on environmental security has also attracted a number of international agreements aimed at protecting the environment.

SELF ASSESSMENT EXERCISE

What is environmental security?

4.0 CONCLUSION

So far, in the last three units including this one, we have explored several forms of security. One revelation about these forms of security is that security as a whole usually involves a network of activities and actions geared toward hazard mitigation, crime prevention and detection, threat mitigation and elimination, risk reduction and management among other objectives. It is therefore, imperative on security practitioners to build synergy through the different functions they perform by working collaboratively on the development of effective security system and management.

5.0 SUMMARY

In this unit, we drew our attention to other forms of security not previously discussed. And we began with the meaning of infrastructure security, and later went ahead to describe seaport security, and subsequently we explained airport security and its elements. Also, we explained food security, health security, economic security and last but not the least was environmental security.

6.0 TUTORED MARKED ASSIGNMENT

Describe on any five of the following forms of security:

Infrastructure Security
Seaport Security
Airport Security
Food security

Health Security
Economic Security
Environment Security

7.0 REFERENCES AND FURTHER READING

Adeboyejo, Thompson A. (1994) "Man's Physical Environment System", in S.K. Balogun (ed.) *Basic Concepts in Society, Government and Economy*, Ibadan: Sam Bookman Ltd.

Alemika, E. E. O. (1997) "Police, Policing and Crime Control in Nigeria" *Nigerian Journal of Policy and Strategy* 12 (1 & 2): 71 - 98.

Greenberg, M. D., Chalk, P., Willis, H. H., Khilko, I., Ortiz, D. S. (2006). *Maritime Terrorism*: *Risk* and *Liability*. Santa Monica: RAND Corporation.

http://ec.europa.eu/agriculture/glossary/index_en.htmm. Retrieved on 30 August 2009.

://en.wikipedia.org/wiki/Port_security. Retrieved on 25 August 2009

://www.aip.org/tip/INPHFA/vol-10/iss-3/p22.html. Retrieved on 29 August, 2009.

://www.tsa.gov/travelers/highway/index.htm. Retrieved on 28 August

://www.pacinst.org/reports/environment_and_security/env_security_and_climate_change.pdf. Retrieved on 29 August, 2009.

.pbs.org/wgbh/rxforsurvival/glossary.html. Retrieved on 29 August, 2009.

.personal.umich.edu/~alandear/glossary/f.html. Retrieved on 30 August, 2009.

UNIT 5

SIMULATION IN SECURITY PLANNING AND MANAGEMENT

CONTENTS

1.0 INTRODUCTION

Simulation can be applied in different ways, and these may include modelling of natural systems aimed at having an idea of possible vulnerability of the system to specific threats or attacks. It can also be applied to insight on the performance of (security) technology for optimization and effectiveness, safety engineering and training. Simply, simulation assists us to identify potential shortcomings or failures in operation that we may later encounter in the discharge of our duties as security experts or professional.

It is important to note that we must be very careful in our choice of information source to be selected for the simulation process. Selection of relevant information is very strategic in arriving at decision on the crucial characteristics and behaviours to select for the process. It is essential to use simplifying approximations and assumptions in simulation activities. In this unit, the reader/student shall be exposed to the meaning and various types of simulation, and show how they can be applied as well as their relevance to security planning and management.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Describe the concept of simulation;

Identify types of simulation; and

Explain the identified types of simulation.

3.0 MAIN BODY

3.1 Meaning of Simulation

Simulation is not a new concept and practice in security. In traditional African society, simulation was often applied by the guards and warriors. For instance, in the traditional Ila-Orangun in present Osun state, Nigeria, after a series of simulation exercise by the community guards, they discovered that offensive attacks may come from enemies without prior notice especially in the middle of the night. Therefore, they decided to dig a trench to surround the entire community, as a booby trap against the enemy(ies) who may wish to launch an offensive attack, and avoid being caught unaware. Other examples may include the old Oyo Empire wall, Kano wall etc. At this juncture, let us draw our attention to the task of this segment of the unit, which is to expose ourselves to some of the existing definitions of the term simulation. Simulation can be defined as

the imitation of some real thing, state of affairs, or process. The act of stimulating something generally entails representing certain key characteristics or behaviours of a selected physical or abstract system" (://en.wikipedia.org/wiki/simulation).

...the act of imitating the behavior of some situation or some process by means of something suitably analogous (especially for the purpose of study) (**Error! Hyperlink reference not valid.**).

....something which simulates a system or environment in order to predict actual behaviour (://en.wiktionary.org/wiki/simulation).

....the process of creating a model (i.e., an abstract representation or facsimile) of an existing or proposed system (e.g., a project, a business, a mine, a watershed, a forest, the organs in your body) in order to identify and understand those factors which control the system and/or to predict (forecast) the future behavior of the system. Almost any system which can be quantitatively described using equations and/or rules can be simulated. The underlying purpose of simulation is to shed light on the underlying mechanisms that control the behavior of a system. More practically, simulation can be used to predict (forecast) the future behavior of a system, and determine what you can do to influence that future behavior. That is, simulation can be used to predict the way in which the system will evolve and respond to its surroundings, so that you can identify any necessary changes that will help make the system perform the way that you want it to (://www.goldsim.com/ Content.asp?PageID=91)

a broad collection of methods used to study and analyze the behavior and performance of actual or theoretical systems. Simulation studies are performed, not on the real-world system, but on a (usually computer-based) model of the system created for the purpose of studying certain system dynamics and characteristics. The purpose of any model is to enable its users to draw conclusions about the real system *by studying and analyzing the model. The major reasons for developing a model, as opposed to analyzing the real system, include economics, unavailability of a "real" system, and the goal of achieving a deeper understanding of the relationships between the elements of the system* (://www.answers.com/topic/simulation).

If we subject the foregoing definitions to operational dissection, you may agree with me that simulation can be used differently by various professions or for different purposes. But, at the beginning of the 20th century, introduction of computer to the world population and the emerging appreciation of systems theory and cybernetic studies unified to a large extent the processes of simulation in various fields. For instance, relevant officials in an Examination body like the West African Examination Council (WAEC) can conduct simulation to test the reliability of various measures put in place by the examination body to curb or reduce examination practices. Emergency workers can also engage in simulation to examine the effectiveness or efficiency of their emergency systems and level of preparedness to responding to emergency situations.

In addition, the police can also conduct simulation exercise to put their preparedness to test on how timely and effectively they can respond to any security threats. They act the simulating scripts as if the situation is real. Frankly, it is no exaggeration that Nigeria police lacks the culture of security simulation. Otherwise, the way the men and officers of the police are being killed on a regular basis from attacks on police stations, armed robbers' bullets or any other threats/hazards would have been very minimal. It is no surprise that police personnel always fail to respond very appropriately and effectively to emergencies. This shows that their level of preparedness is very far below the average. This is one of factors responsible for the call being made by concerned citizens, for the introduction of joint patrol that would be composed of members of police and the armed forces especially the Army.

Simulation can be facilitated with computer in health-care, military, or education simulation or any other sector. A lot of simulation software have been invented, having the user to decide on which one will fit into the purpose for which the simulation is to be carried out.

SELF ASSESSMENT EXERCISE

What is simulation?

3.2 **Types of Simulation**

The importance of simulation in strategic security planning and management cannot be over-emphasised, especially as it concerns identifying any weakness in our systems and operation through which we can develop alternative ideas and policies to address such weakness and vulnerability to mitigate the risk of system or/and operational failure. As we have rightly pointed out earlier, simulation can be used for numerous purposes depending on the problem we want to unravel and apply solution to.

The complexity of the problem we are working on may require a simulation package or exercise that will demand from us, a very sound knowledge on how to apply the tool(s). In this case, the services of experts may be required to guide the simulation process if the application is a (very) technical one. Let us go back to the basis of this segment of the unit, which involves explaining various types of simulation. Basically, types of simulation may include the following:

(a) Education and Training Simulation: The security profession requires sufficient mental alertness and physical strength, and that is why it is not everybody that can hold a security job. The nature of the security profession underscores the need by professionals to engage themselves in periodic training. For instance, it is very sad to hear such situations where police pursue armed robbers and fail to pin down the bandits despite the numerical strength and strategic advantage the police ought to have over them. Sometimes, the bandits appear to be more equipped than the police as a result of operational failure on the part of the police. Situations like these undermine the relevance of the public security personnel's capacity to maintain law and order as well as check any acts of criminality (Onyeozili, 2005: 40).

Also, the problem of police team being overpowered by the sophistication of the weapons that robbers carry can be easily addressed if the men and officers of the police undergo simulation exercise from time to time. Even members of patrol team should simulate before going out to discharge their duties, so that they can weigh their vulnerability against their capacity for optimal performance. If they can identify areas of vulnerability in their operations, they can then map out strategies to build their capacity towards preventing the threats from happening or mitigating the effects, that such threats can have on them or their operation when and where they occur.

For instance, a security patrol team that receives a signal that a bank robbery is going on in a place will be expected to act immediately to foil the robbery. But, most times, police patrol (rescue) teams are in the habit of announcing their (the police) coming to the robbers through the blowing of sirens. Unfortunately, before they reach the location of the robbery, the robbers would have laid ambush for them, a situation which often forces the lucky policemen to retreat, as they always find it difficult to recover promptly due to lack preparedness in hazard mitigation and strategic planning.

Where security men simulate, their preparedness level against any attack will be very high because this would have projected into the future and identified potential threats or challenges that may be encountered in the course of discharging duties as a security professional. And in doing this, you will prepare yourself before hand, and in the event that such hazard or attack occurs the losses that may be recorded will be minimal. I feel it is more appropriate for the police not to alert the robbers of their coming through blowing of siren. This is because the daring nature of most armed robbers in the country has made blowing of siren by law enforcement agents obsolete. They are die-hard and always willing to challenge the law enforcement agents in gun battle. Strategically, for the fact that the rescue team do not know the identities of the bandits, it is better that they send an intelligence team to do some collation of vital information about the happening in the affected area for situation analysis.

After conducting situation analysis, we need to conduct risk analysis and assessment to know if it is most appropriate to move straight into where robbery is taking place or it is most reasonable to block all roads that lead to the affected location and wait for the robbers to come out. The reason for this process is to avoid fatality or loss of lives especially civilians that may be hit by strong bullets in the course of engaging the bandits.

After conducting a risk assessment, it may be agreed that a team should be sent to the scene, all members of whom should be in plain-cloths, so that they cannot be easily identified by the robbers. But, if it is considered that the robbers will do more harm by being allowed to complete their operation before attacking them, a team of experienced officers and men may be sent in.

Caution should be exercised here as there is the need to equip the policemen and officers with bullet-proof vests because people are not applying for security profession with the ultimate desire to suffer avoidable death. The use of tear-gas may be required to make the robbers lose their balance and destabilise them. I feel, here is the most convenient place to stop our discussion on ways to foil or liquidate a robbery incident. As you may know, we cannot exhaust all aspects of security discourse in a forum. Security requires continued research and intellectual probing.

By and large, education simulation helps us to know the most appropriate training (academic or fitness) we need to undertake to optimise our performance in the discharge of our duties as security experts and professionals. There is no doubt, security professionalism is very tasking considering the hazards and work overload that characterise it. Security personnel work long hours that sometimes they hardly have time to attend to personal issues. It is pertinent for policy makers to see education simulation as important element of security sector reform (SSR).

There are three types of education and training simulation. The first one is **live simulation**. In live simulation, it is expected that trainees use stimulated or mannequin equipment in the real world. As you may be aware, it is not all security trainings that can be undertaken with the real equipment. For instance, if a training is going to be conducted in knowing how effectively, each of your security officers can act in the face of hazard or in shoot-outs with criminals (terrorists, militants, armed robbers etc), one cannot expect that those trainees should be equipped with live ammunitions because of the risk involved in such action.

It might not be wise to allow the use of real weapons for training due to the possibility of recording avoidable deaths among the trainees. It is, therefore, advisable to use live simulation through which we can still know the level of competence of each trainee without putting them to unnecessary risk of killing themselves. In the process, the trainees will identify their individual and collective areas of vulnerability and subsequently develop ways through which they can improve on their capacity for optimal performance.

It is unfortunate that in Nigeria, security personnel, most times, are posted to specific positions without considering their level of competence for the job or assignment. For instance, officers of the armed forces lobby to be included in peacekeeping contingent without training on simulation, which can help in making them aware of the inherent risks involved in undertaking peacekeeping mission in troubled zone(s), and be well-prepared psychologically, physically, emotionally and strategically. Many soldiers lose their lives after being seduced with ladies by the enemies. Live simulation is also known as “high fidelity”. This demonstrates the samples of the (possible) real performance of the trainees compared to the “low fidelity” simulation that is based on the use of pencil and paper that can only show “signs of performance” (**Error! Hyperlink reference not valid.**) rather than the practical performance of the trainee(s).

The second type of simulation is **virtual simulation**. Virtual simulation actually involves the use of real people using simulated tools in a simulated world. In virtual simulation, the process often involves the use of computer simulation by the trainees in undergoing training. Virtual simulation usually involves security employees training in an artificial environment (generated through computer software), and take it as if it is real. The exercise is undertaken through the manipulation of the computer keys or mouse. Virtual simulation is often facilitated through sight and sound.

The third type is **Constructive simulation.** Constructive simulation usually involves a process whereby simulated people use simulated tools in a simulated world. This simulation type is also known as war-gaming. It can be described as a form of simulation whereby “players command armies of soldiers and equipment that move around on around on a board” (**Error! Hyperlink reference not valid.**). We shall discuss this type of simulation extensively subsequently (see military simulation);

(b) Health Care Simulation: This form of simulation is also in security and safety. It affords health care providers an opportunity to examine their capacity to respond to emergency situations. Simulation helps to reduce the situation of crisis in patients because, as stressed by Eder-Van Hook (2004):

A health care provider's ability to react to prudently in an unexpected situation is one of the most critical factors in creating positive outcome in medical emergency, regardless of whether it occurs on the battlefield, freeway, or hospital emergency room (cited on ://en.wikipedia.org/wiki/simulation).

Eder-Van Hook stressed further, saying that medical errors or lack of adequate medical attention to patients by health care providers have led to almost ninety-eight thousand (98,000) deaths, with a lot of financial implications, which amounts to between $US37 and $US50 million on an annual basis. It is very unfortunate the way health-care providers in Nigeria respond to emergency cases. For instance, somebody who is shot by a group of robbers will hardly survive the bullet wounds he/she sustains from the bandits. The issue is not basically because he/she has been shot in part(s) of the body and can hardly survive but the poor handling of the situation always results in high rate of avoidable deaths in our hospitals.

It is a very abnormal situation for some patients in teaching hospitals to be given referral to private clinics for treatment, and the reason always given is lack of competent medical hands that can manage the medical needs of these poor patients. What a situation like that denotes is that our teaching hospitals can no longer be considered as tertiary health-care institutions as they have relegated their responsibilities (in the name of making money) and transfer such to private clinics many of which can hardly boast of having enough qualified medical staff. In this kind of messy situation, health-care simulation will make no sense to the health practitioners because many of them have found it more important to make brisk business than saving lives. Sadly, the decision makers that are supposed to caution them are less bothered because they can afford treatment abroad most times.

Bringing our attention back to the subject under discourse, health-care simulation has been demonstrating growing relevance in the modern medical world. Several medical simulations usually involve connecting computer to a plastic simulation of related anatomy e.g. the use of dummy that reacts to injected drugs and can also be automated to generate simulations of life-threatening emergency situations or cases. In some instances, the simulation procedures are captioned and reproduced by computer graphics tools. Health-care simulation has continued to be found useful in training medical practitioners on the ways to build their individual and collective capacities in responding effectively and timely to emergency situations especially as regards the issue of saving lives and management of health crisis; and

(c) Military simulation is also known as war-gaming. It involves an act of simulating with the intention of putting various theories of war into test and if need be, refine those theories without undergoing the real hostility of warfare. The rationale behind military simulation is to facilitate a process through which one can arrive at tactical, strategic and doctrinal answers to problems that bother on defence and warfare. War-gaming can be described as a form of game or hobby that showcases various activities of military operation in a simulated environment.

War-gaming can be used for relaxation or game-playing, and this is known as conflict simulations or consims. But, if we desire to engage in war-gaming for the purpose of warfare, the process is usually known as war-game or military exercise. Meanwhile, those that engage in war-gaming as a hobby don't usually draw any distinction between the two aspects of warming earlier mentioned because they always contend that whether for war-making or relaxation, any war-game should demonstrate to a large extent characteristics of human behaviour as it would be have been in the real world when war is being conducted (see .alanemrich.com/PGD/Week_03/PGD_what_is_a_War game.htm.

However, war-game can be classified as historical, hypothetical, fantasy, or science fiction. **Historical war-games** are often modelled after real events and putting into simulation reasonable approximations of the actual forces, terrain as well important factors that represent the experience of the real players or participants. For instance, those who usually have experience of Play Station (game) especially the soccer, will notice that each of the players demonstrates the real capacity of the model player(s).

In Play Station 2, the scoring ability of Christian Ronaldo (formerly of Manchester United FC of England, but now of Real Madrid FC of Spain) cannot be compared with his scoring ability in Play Station 3, there being tremendous improvement in his scoring ability. Play Station 3 reflects the improvement in his scoring ability, showing that the simulated Christian Ronaldo demonstrates the actual ability of the real Ronaldo as at the time the programme or application was being written. Here, the history of the performance and experience of players is considered in determining the capacity of the simulated players.

Hypothetical war-games are actually those games that involve drawing simulating materials about wars that did not happen. **Fantasy and science fiction war-games** usually involve developing games from wars generated from works of fiction or (creative) imagination. There are more types of simulation but the three we have discussed in this unit can be considered as the basic types of simulation for security planning and management. The reason is that they cover virtually all aspects of securitisation namely disaster management, law enforcement, defence, warfare, to mention a few.

SELF ASSESSMENT EXERCISE

Explain types of simulation.

4.0 CONCLUSION

In the final summation of our discourse on the concept of simulation, the concept can be described as an essential instrument of decision analysis. It affords us a great opportunity as security experts or practitioners to know the various areas of deficiency in our service delivery, operations as well as potential threats. The relevance of simulation in modern security planning and management is enormous owing to the nature of uncertainty that characterises the general affairs including security issues in recent times. For instance, since the end of the Cold War, state actors have constituted less threat to national and international security compared to the destructive attitude portrayed by some non-state actors, which absolutely undermine the potentials of the security sector to maintain law and order.

The event of September 11 2001 terrorist attack in the US has shown the very destructive dimension that threat emanating from non-state actors has assumed. Prior to that ugly incident, we could hardly conceive the idea that commercial planes could be used as weapons of mass destruction. There is no doubt, simulation assists us to appraise and compare among alternative designs, plans and policies, so that we can choose those that will enable us achieve optimal performance for best results. Simulation is very vital in security planning due to its capacity to unravel secrets of uncertainties and guide us in deriving solutions to the problem of uncertainty that can affect our operations and policy-actions as security professionals in a quantifiable way. Above all, simulation provides us an avenue to explore ways through which we can improve on our preparedness for risk and hazard mitigation and high recovery capacity in the event of any hazards or threats.

5.0 SUMMARY

In this unit we explored some of the existing definitions of the concept ‘simulation’. One fact that appeared from the various definitions presented, shows that simulation can be applied in various fields or disciplines and for different purposes. We have therefore discussed some of the basic types of simulation that can be employed in security planning and management in order to safeguard the security of people as well as their property. I hope that you have found this unit as interesting as you expected it to be. If you have any question on any aspect of this unit or the course in general, please feel free to get in touch with the instructional and tutorial facilitator. Good luck.

6.0 TUTOR MARKED ASSIGNMENT

What is simulation?

Write short note on three types of simulation.

7.0 REFERENCES AND FURTHER READING

://en.wikipedia.org/wiki/simulation. Retrieved on 25 August 2009.

://en.wiktionary.org/wiki/simulation. Retrieved on 25 August 2009.

Error! Hyperlink reference not valid.. Retrieved on 25 August 2009.

://www.alanemrich.com/PGD/Week_03/PGD_what_is_a_Wargame.htm. Retrieved on 14 April, 2008.

://www.answers.com/topic/simulation. Retrieved on 24 August 2009.

://www.goldsim.com/ Content.asp? PageID=91. Retrieved on 24 August 2009,

Error! Hyperlink reference not valid.. Retrieved 25 August 2009.

MODULE 2

UNIT 1

MEANING & TYPES SECURITY THREAT I: NATURAL THREATS

CONTENTS

1.0. INTRODUCTION

The meaning of security has been generating a great debate among scholars in recent times. There has been a call on government at all level to change the operational direction in the management of security in their various domains. Initially, apart from natural hazards, major threats that confronted every nation were thoese emanating from state actors. The security of communities were being undermined through invasion, reprisal attacks or war of solidarity where two or more communities or countries came together to confront and challenge the hegemony of a powerful community or nation. One major fundamental objective of war of solidarity is embarking on policy of aggression with the utmost desire of actualising balance of power where no community or nation will be considered too powerful, knowing the implication of such power on the political and territorial sovereignty of the neighbouring communities or countries.

It is no gainsaying, with the contemporary experience of security situations in world politics, to assert that there is a paradigm shift in security discourse. Recent experiences show that major threats often come from other sources other than the state actors. The role of resource scarcity in undermining the general security and challenging the political sovereignty of any nation underscores the tendency of situation of poverty and deprivation can generate disorder and insecurity in any community or state. In this unit, we shall be defining security threats and further discussing the natural threats as manmade threats shall be explained in the next unit.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Explain the meaning of security threat;

Identify types of natural threats; and

Examine the major types of natural threat

3.0 MAIN BODY

3.1 **Meaning of Security Threat**

Waever (1995) associates the concept of security threat to security problems that undermine the security of any nation or community, and relates it to various "developments that threaten the sovereignty or independence of a state in a particularly rapid or dramatic fashion, and deprive it of the capacity to manage by itself. This, in turn, undercuts the political order. Such a threat must therefore be met with the mobilization of the maximum effort" (Waever, 1995: 54). Similarly, security threat can be described as the capacity of any human or non-human element to destroy the vital interests of others considered as targets. Security threat also means:

......*a party with the intent and capability to exploit a vulnerability in an asset. This could be a malicious hacker or a disgruntled employee* :/ /proxy.11a.nu/2006 /02/ 11/definition-of-risk-vulnerability-and-threat).

.......*an explicit or implicit message from a person to another that the first will cause something bad to happen to the other, often except when certain demands are met. Often a weapon is used. Examples are a robbery, kidnapping, hijacking, extortion, blackmail* (://www.knowledgerush.com/kr/encyclopedia/Threat).

........*anything that threatens the residents of a community or the things they value* (Gordon, 2000).

..........*are persons, things, events, or ideas, which pose accidentally or deliberately some degree or danger to an asset.* (US National Institute of Standards and Technology cited in Kuban & MacKenzie-Carey, 2001).

Dissecting the foregoing definitions of the term security threat, you will conclude that security threat covers all aspects of any malicious intention or action or occurrence geared towards making a party vulnerable and exposed to security risk. Security threat can simply be divided into two, namely natural and manmade threats. The former are usually generated by nature while the latter involve cruel attacks arising from human actions and behaviour. The manmade threats involve malicious activities of man, which may include armed robbery, assassination, computer intrusion, information hacking and corruption, violent behaviour, ethnocentrism, religious bigotry, terrorism, to mention a few.

Meanwhile, our focus in this unit, apart from explaining the meaning of security threat, is to explain the major natural threats to security. As a matter of fact, there are several forms of natural threats to security and in this segment we shall be discussing some of these threats. Natural threats can be divided into two, namely minor and major. Examples of these major natural threats include hurricane (cyclone), earthquake, drought and flood. On the other hand, those natural threats or hazards considered to be minor may include cold wave, storm, mudslide, thunderstorms, to mention a few. However, we shall be focussing on the major natural threats or hazards, and you are advised to engage in further reading or independent study, and make sure you source for the meaning of the various minor natural threats or hazards.

3.2 Types of Natural Security Threat

A natural disaster is the consequence of a natural hazard. If there are no measures put in place towards hazard mitigation, there is likelihood for such hazard to result in disaster. Thus, disaster involves massive loss of lives and/or property to hazardous situation or attack. Example of natural hazards may include earthquake, flood, volcanic eruption, landslide, to mention a few. We shall begin to discuss them one after the other.

3.2.1. Earthquakes

Mythologically, earthquake was believed among the Greek to be caused by Poseidon the god of earthquake. It was argued Greek mythology that whenever Poseidon was in a state of sadness, he would smack the land with a trident, causing the earth to quake. It was claimed that this god also used earthquake as a tool of fear, warning people of the damaging effect of his punishment on men and their environment(s), as a way of admonishing men not to offend him (see Sellers, 1997).

Conceptually, an Earthquake is an unexpected and hazardous vibration resulting from the sudden shake of the Earth's crust. The degree of the vibrations may differ. An earthquake can be said to have two points. The first point concerns the “.... point of origin underground”, and this is known as “focus” while the second point is usually “directly above the focus on the surface”, and it is regarded to as the “epicentre” (://en.wikipedia.org/wiki/Earthquake).

One unique character of the earthquake is that it does not constitute any danger to people or animals on its own, but its consequences such collapse of building and electric poles, electric shock, fire, to mention a few usually cause harm to people. This means that it is imperative to have safety measures in place and encourage hazard mitigation as the best practices to avoid disaster. Let us consider some other definitions of earthquake.

An earthquake (also known as a tremor or temblor) is the result of a sudden release of energy in the Earth's crust that creates seismic waves. Earthquakes are recorded with a seismometer, also known as a seismograph (://en.wikipedia.org/wiki/Earth quake).

Sudden motion in Earth caused by abrupt release of slowly accumulated strain. Shaking of the Earth caused by a sudden movement of rock beneath its surface .Geocities.com/seiswash/terms_and_definitions.htm

It is the rupture of geological faults that often causes earthquake but nuclear experiments, landslides, mine blasts as well as volcanic activity can also provoke the earth to quake. Some of the incidents of earthquake include the 2004 Indian Ocean earthquake, which was the second largest earthquake in history. The attendant tsunamis occasioned by this earthquake affected several countries including Pakistan and India, leading to the death of over two hundred thousand people. There is no doubt that the effects of earthquake can be very devastating not only to man but also the general ecosystem. Some of these effects include the following:

(a) Tremulous shaking of land and ground ruptures. These are the major effects of earthquake, leading to serious damage to buildings and other rigid structures like bridges, street lights and their stands, electric poles, bill boards, among others. The amount of damage and destruction that will be occasioned by the incident of earthquake depends largely on the complex combination of the earthquake magnitude, the distance from epicentre as well as the geological and geomorphologic conditions that may magnify or lessen wave propagation (see ://www.abag.ca.gov/bayarea/eqmaps/doc /contents.html). However, ground acceleration is usually used in measuring the degree of ground shaking.

(b) Fires: Another effect that can be caused by earthquake is the occurrence of fires. After the shaking, a lot of structures and building get damaged or destroyed including petroleum/gas pipelines and facilities. As earlier mentioned, the quake can also uproot electric-pole and damage power-lines, and in the process, spark from the power-line or electric-poles may come in contact with gas or petrol to generate fire. The pressure of these fires may be high and thereby be very difficult to contain them. An example of where the earthquake caused lesser threat than its fire outbreak effect was 1906

San Francisco earthquake where many people died as a result of the fires that accompanied the earthquake incident (see **Error! Hyperlink reference not valid.**)

(c) Soil liquefaction: One of effects of earthquake is soil liquefaction, which involves a situation whereby soil losses its firmness and transforms from solid to liquid. The situation is caused when water-saturated granular material like sand losses it strength and in the process its solidity becomes liquid, resulting in the sinking of buildings because the soil does not have strength to carry the weight of these structures any longer due to the quake of the earth such as experienced in the 1964 Alaska earthquake (**Error! Hyperlink reference not valid.**);

(d) Other effects of earthquake may include tsunami and flood, which will be discussed later in this unit, as well as massive destruction of lives and property. Earthquake can also lead to outbreak of diseases and food insecurity resulting from the damage.

SELF ASSESSMENT EXERCISE

How do you define earthquake as a natural threat to security?

What are the effects of earthquake?

3.2.2. **Hurricane**

In the last twenty years, there has been huge amount of losses in human and material terms through incidence of hurricane, though, the problem is less visible in sub-Saharan Africa compared to Asia, Oceania, North America, among others. For instance, the destruction that emanated from Hurricane Andrew (1992) alone was "estimated at more than $25 billion in South Florida and Louisiana and undoubtedly would have been higher had the storm hit Miami directly" (://hurricanes.noaa.gov/pdf/hurricanebook.pdf). For the sake of conceptual clarity, let us at this juncture explore some of the existing definitions of hurricane. What is a hurricane?

A hurricane is a type of tropical cyclone, which is a generic term for a low pressure system that generally forms in the tropics. The cyclone is accompanied by thunderstorms and, in the Northern Hemisphere, a counterclockwise circulation of winds near the earth's surface (://hurricanes.noaa.gov/pdf/hurricanebook.pdf).

A hurricane is an intense, rotating oceanic weather system that possesses maximum sustained winds exceeding 119 km/hr (74 mph). It forms and intensifies over tropical oceanic regions. Hurricanes are generally smaller than storms in mid-latitudes, *typically about 500 km (311 miles) in diameter. At the ocean's surface, the air spirals inward in a counterclockwise direction. This cyclonic circulation becomes weaker with height, eventually turning into clockwise (anticyclonic) outflow near the top of the storm* (://www.comet.ucar.edu/nsflab/web/hurricane/311.htm).

Source: ://www.why-is-the-sky-blue.tv/what-is-hurricane.htm

Hurricanes emanate and build-up over oceanic regions. They usually entail sea-surface temperatures of at least 26°C (80°F) as well as "the influence of the earth's rotation to initiate a spinning circulation (Coriolis effect)" (**Error! Hyperlink reference not valid.**). There are four phases to the incidence of hurricane. The first phase usually involves tropical disturbance evident in the rain clouds such that moist air increases and becomes cooler. The second phase is characterised by tropical depression with thunderstorms. Here, there will be low pressure-winds with circular patterns. The third phase consists of tropical storm, which usually involves wind that travels 38 mile per hour, occasioning storm clouds and rough sea. At this stage, one does not need to be told of the impeding danger. The last phase finally welcomes the incidence of hurricane itself, featuring wind that moves at 74 miles per hour and heavy rainfall. At this stage, hurricane will get to its climax. It is important to note that hurricane is given different names in other places, and these names may include tropical cyclone and typhoons (see table 1.1):

Table 1.1: Hurricane and Its other Names in Different Parts of the World

Hurricanes	North Atlantic Ocean, Caribbean Sea, Northeast Pacific Ocean and the Gulf of Mexico
Typhoons	Northwest Pacific Ocean
Tropical cyclones	Australia and the Indian Ocean

Effects of Hurricane

Hurricanes have destructive effects, and these effects may include storm surges, inland flooding and tornadoes. Several lives and property have been lost resulting from inland flooding, even more than the hurricane itself. The storm corrodes beaches, destroys coastal highways and erodes house foundations. Hurricanes create destructive surface winds and storm surges. High winds bring about huge structural and environmental damage, as the storms are usually the most destructive component of a hurricane.

A storm surge actually involves a rise in the level of the sea along a coastline necessitated by the combination of a hurricane's surface winds and physical geography of a coastline. The surface winds above the surface of the ocean drive water towards the hurricane's eye, mounting a mound of water. The mound of water is provoked by the slope of the coastline as the hurricane comes close to land. In a situation whereby the coastline is shallow, it will be difficult for water to flow away from the mound and the mound grows. But, if the coastline is deep, then water can easily "disperse and the mound may grow slowly or disperse depending on hurricane strength" (://www.comet.ucar.edu/nsflab/web/hurricane/311.htm). The destructive level of any hurricane depends largely on the attendant wind speed and storm surge (see Table 1.2)

Table 1.2: The Saffir-Simpson Hurricane Intensity

Category	Wind Speed		Storm Surge		Damage
	km/hr	mi/hr	m	ft	
1	119-154	74-95	1-2	4-5	Minimal
2	155-178	96-110	2-3	6-8	Moderate
3	179-210	111-130	3-4	9-12	Extensive
4	211-250	131-155	4-6	13-18	Extreme
5	>250	>155	>6	>18	Catastrophic

Adapted from ://library.thinkquest.org/03oct/00795/hurricanetypes.html

SELF ASSESSMENT EXERCISE

How do you describe hurricane?

3.2.3 **Flood**

Flood is another type of natural threat. It usually involves submerging of land by overflowing water. Flood goes beyond having volume of water like river or lake running off its normal boundaries to cause flooding, but also involves a situation whereby the overflow is engineered by tide. Natural hazards like hurricane and earthquake have the tendency to provoke flood in the affected community. Let us quickly define flood. In doing so, we shall be considering the definition of the term as presented by various sources. Thus, flood can be described as:

......a general or temporary condition of partial or complete inundation of normally dry land areas from overflow of inland or tidal waters or from the unusual and rapid accumulation or runoff of surface waters from any source (**Error! Hyperlink reference not valid.**).

....the rising of a body of water and its overflowing onto normally dry land (://wordnetweb.princeton.edu/perl/webwn?s=flood).

The phenomenon of flood is becoming increasing in Africa and elsewhere due to climate change and environmental pollution. The incident of significant variability in climate has been attracting growing attention among the world population in recent times owing to its impact on man and his/her environment. The trapping of the atmosphere with CO_2 has been the major cause of climate change.

Types of Flood

a) Riverine floods: These can be divided into slow kinds and fast kinds. Slow kinds usually involve water overflow generated by high rainfall or huge fall of snow melt, which goes beyond the capacity of a river's channel. The factors responsible for this kind of riverine floods may include heavy rainfall, monsoons, hurricane and tropical depression, among others. Similarly, these floods that also be caused by unexpected drainage obstruction through dumping of refuse in canals, landslide or even ice. In Nigeria, the problem is basically as a result of incessant dumping of debris in canals and building structures on water passages, obstructing water-flow. On the other hand, fast kinds are experienced as a result of "convective precipitation (intense thunderstorms) or sudden release from an upstream impoundment created behind a dam, landslide, or glacier" (://en.wikipedia.org/wiki/Flood);

b) Estuarine Floods: They are normally caused as a combined effect of sea tidal surges necessitated by storm-force winds from either a tropical cyclone or an extra-tropical cyclone;

c) Coastal floods: These are floods generated by severe sea storms or due to a destructive hazard like hurricane or tsunami; and

d) Catastrophic floods: These kinds of floods are initiated by accidental dam breakage or earthquake or volcanic eruption, capable of creating huge destruction of lives and property.

Effects of Floods

a) Destruction of infrastructure and other physical structures: Effects of Floods particularly the severe ones include destruction of houses, sewer systems, bridges, schools, to mention a few;

b) Casualties: The incidence of floods can result in the loss of lives and livestock. It is capable of creating epidemic in the affected communities;

c) Shortage of water: As a result of contamination of water, there may be (acute) shortage of portable water;

d) Loss of Environmental sustainability: Incidence of flood can lead to shortage of resources because of the effect that such floods may have on the development of affected communities. In the process of flooding, many farms might be destroyed, and food shortage will be imminent except there is intervention of food supply to the affected communities by government or emergency agencies and donors; and

e) Outbreak of disease(s): The event of flood can generate an outbreak of diseases in the affected community. For instance, there is possibility of experience water-borne diseases like cholera, where sewer systems have been destroyed by flood.

SELF ASSESSMENT EXERCISE

Write short note on the meaning, types and effects of flood.

3.2.4 **Drought**

Drought is actually a normal climatic situation. It is experienced in almost all parts of the world, but it can constitute a security threat if its occurrence is significant. This is because it is supposed to be a temporary condition, which should not last for too long. Drought appears to be another hazard that can lead to disaster if its effects are not mitigated by the people or concerned communities. It is no gainsaying that it can exacerbate condition of hunger in any community due to food shortage resulting from poor agricultural yields. Meanwhile, drought goes beyond agricultural condition, and it is imperative at this juncture, to look at some of the definitions of the term, drought.

A drought is an extended period of months or years when a region notes a deficiency in its water supply. Generally, this occurs when a region receives consistently below average precipitation. It can have a substantial impact on the ecosystem and agriculture of the affected region (://en.wikipedia.org/wiki/Drought).

Drought is an insidious hazard of nature. Unlike many disasters which are sudden, droughts result when there is less than normal precipitation over an extended period of time, usually a season or more. The decreased water input results in a water shortage for some activity, group, or environmental sector. Drought can also occur *when the temperature is higher than normal for a sustained period of time; this causes more water to be drawn off by evaporation. Other possible causes are delays in the start of the rainy season or timing of rains in relation to principal crop growth stages (rain at the "wrong" time). High winds and low relative humidity can make matters much worse* (IFAS, 1998: 1).

Bearing in mind the foregoing definitions, you may agree with me that the problem of drought becomes evident especially when man's demand for water grows at geometric progression and reduction in the volume of water supply is also experienced at geometric progression. At this point, the incident of drought can lead to disaster except adequate interventionist measures and mitigation initiatives are brought to bear. There is no doubt that the incidence of drought exists everywhere, particularly where there is high usage of water. This hazard has the potentials of undermining the economic and environmental security of any society. The problem is very evident in Africa due to lack of adequate preparedness and mitigation strategies (irrigation, crop rotation and environmental protection) to reduce the impact of the risk that drought poses to environmental sustainability and economic wellbeing of the people.

Types of droughts

a) Meteorological drought: This is a form of drought effected by a long absence of normal precipitation. Here, the period is greeted with precipitation that is below average. This type of drought is the first drought that can be experienced before other forms of drought emerge. Therefore, it provides a kind of warning-signal to the affected communities of the impeding risk;

b) Agricultural droughts: These are droughts that propel poor yields in farm cultivations. They have adverse effect on crop production and can lead to food insecurity in the affected community; and

c) Hydrological droughts: These usually mount environmental security threat to people by reducing the level of water in water reserves like aquifers, lakes and reservoirs, such that the water level will be short of the statistical average. In a situation like this, the possibility of having (acute) water shortage is very high.

Effects of droughts

a) Poor agricultural yields and crop production which can lead to food insecurity, of which food insecurity is usually accompanied by starvation and hunger, which can also generate political tension, violence, and increase in crime rate among other security risks;

b) Forced migration: Droughts can also propel a situation of migration among the people of any affected community to another place in search of arable land for cultivation or greener pasture. In a situation whereby the host community cannot provide the visitors the needed opportunities to actualise their hopes, may be due to prevailing socio-economic and political circumstances in the host community, there is tendency that the immigrants will look for alternative means to survive, some of which can constitute a greater security threat to the hosts. A good example is the migration of several Tuareg from Niger Republic to many states in northern Nigeria especially Kano due to endemic droughts being experienced in their home country.

The rapid migration of these foreigners from neighbouring countries has been said to be a major cause of increasing incidence of religious violence in the north especially Kano, Borno and Bauchi states. It was no surprise in the *Akaluka* religious riot in Kano, that out of several rioters arrested by security operatives in Nigeria, only one was Nigerian while others were foreigners notably from neighbouring Niger Republic (see Albert, 1999: 292). This situation shows the amount of threat that droughts can pose to the security of any nation;

c) Famine: Droughts can also generate famine due to lack of water for irrigation. Drastic reduction or absence of water as occasioned by droughts, will definitely affect farming adversely, capable of generating scarcity of food (famine);

d) Disease outbreak: Droughts can also provoke a situation of Malnutrition, dehydration and related diseases due to shortage in water supply for agriculture and human consumption; and

e) War and Violence: Resulting from the problem of environmental resource scarcity caused by droughts, there may be growing struggle among the people to compete for the available lean resources, which cannot go round. Therefore, people will live under harsh conditions adorned with the attitude of survival of the fittest, which creates violence and hostilities especially where there is sharp ethnic division with patron-client ideology. Other effects may include increase in the incidence of snakebites as experienced in drought-ridden areas in northern Nigeria and elsewhere (see ://news.bbc.co.uk/2/hi/asia-pacific /6282075.stm), desertification and erosion, social unrest and criminality, and wildfires, to mention a few.

SELF ASSESSMENT EXERCISE

How do you describe drought as a security threat?

4.0 CONCLUSION

It is a truism that the capacity of any community to respond to hazardous situations depends largely on its resilience and preparedness towards risk reduction and hazard mitigation. The recovery capacity of any community, wishing to mitigate the effect that the occurrence of any hazard may have on her and its people, must be substantial enough to withstand the threat or hazard. If no efforts are made to mitigate or reduce the impact of hazard or attack, there is the possibility that such hazard will result in disaster. It is therefore important for stakeholders to adopt strategies through which they can improve their capacity to respond to hazardous situations timely and effectively. A fact that comes out of this intellectual standpoint is that disaster does not usually occur where vulnerability is low or absent.

Take for instance, in Nigeria, the problem of flood would have been minimised if government had put in place measures and adopted policy actions that mitigate risk emanating from environmental degradation and deforestation, which form part of the causes of flood. The culture of deforestation has continued to be evident especially from the felling of trees as firewood for cooking. The problem is that households especially those in rural settings cannot afford the exorbitant cost of kerosene and cooking gas to do their cooking. Therefore, many have resulted in the use of firewood, a situation that can be a driving force for the incidence of flooding. The problem of climate change is becoming phenomenal considering its adverse impact on environmental sustainability of every nation especially the developing countries.

5.0 SUMMARY

In this unit, we focussed on the meaning of security threat. After defining the term security threat, we also identified the two types of security threat to include natural threats such as earthquake, flood etc, and manmade threats including robbery, terrorism, war, etc. Thereafter, we explored the meaning of natural threat and various major natural threats or hazards. In the next unit, our searchlight shall be beamed on manmade threat and its various forms. I have no doubt that you have found this unit very thought-provoking and decipherable.

6.0 TUTORED MARKED ASSIGNMENT

What is security threat?

What are the basic types of security threat that you know?

Briefly explain any three natural threats that you know.

7.0 REFERENCES AND FURTHER READING

Albert, I.O. (1999). Ethnic and Religious Conflicts in Kano. In: Otite, O & Albert, I.O (eds.). *Community Conflicts in Nigeria: Management, Resolution and Transformation*. Ibadan: Spectrum Books Ltd & Academic Peace Associates Work, Abuja, Nigeria. 274-309.

Gordon, J. (2000). Risk Assessment and Management in Local Government Emergency Planning, Part 1: Basic concepts. *Canadian Journal of Emergency Management* 2(2): 11-12.

Institute of Food and Agricultural Sciences (IFAS) (1998). Extreme Heat and Drought. In *the Disaster Handbook*. Florida: University of Florida (Chapter 16). Also available on ://disaster.ifas.ufl.edu/PDFS/CHAP16/D16-05.PDF. Retrieved on 1 September, 2009.

Sellers, Paige (1997). Poseidon. *Encyclopedia Mythica*. Available on **Error! Hyperlink reference not valid.**. Retrieved on 2 September 2008.

US National Institute of Standards and Technology cited in Kuban, R. & MacKenzie-Carey, H. (2001). *Community-Wide Vulnerability and Capacity Assessment*. Office of Critical Infrastructure Protection and Emergency Preparedness, Canada.

Waever, Ole (1995). Securitization and Desecuritization. In: Lipschutz, R.D (ed.). *On Security*. New York: Columbia University Press. 46-86.

Error! Hyperlink reference not valid.. Retrieved on 30 August, 2009.

Error! Hyperlink reference not valid.. Retrieved on 30 August, 2009.

://en.wikipedia.org/wiki/Drought. Retrieved on 30 August, 2009.

://en.wikipedia.org/wiki/Earthquake. Retrieved on 30 August, 2009.

://en.wikipedia.org/wiki/Flood. Retrieved on 30 August, 2009.

://hurricanes.noaa.gov/pdf/hurricanebook.pdf. Retrieved on 30 August, 2009.

://library.thinkquest.org/03oct/00795/hurricanetypes.html. Retrieved on 30 August, 2009.

://news.bbc.co.uk/2/hi/asia-pacific/6282075.stm. Retrieved on 30 August, 2009.

://proxy.11a.nu/2006 /02/ 11/definition-of-risk-vulnerability-and-threat). Retrieved on 30 August, 2009.

://www.abag.ca.gov/bayarea/eqmaps/doc/contents.html. Retrieved on 30 August, 2009.

://www.comet.ucar.edu/nsflab/web/hurricane/311.htm. Retrieved on 30 August, 2009.

.geocities.com/seiswash/terms_and_definitions.htm. Retrieved on 30 August, 2009.

://www.knowledgerush.com/kr/encyclopedia/Threat. Retrieved on 30 August, 2009.

Error! Hyperlink reference not valid.. Retrieved on 30 August, 2009.

://www.why-is-the-sky-blue.tv/what-is-hurricane.htm. Retrieved on 30 August, 2009.

://wordnetweb.princeton.edu/perl/webwn?s=flood. Retrieved on 30 August, 2009.

UNIT 2

MEANING & TYPES OF SECURITY THREAT II: MANMADE THREATS

CONTENTS

1.0. INTRODUCTION

In the last unit, our study centred on the meaning of security threat, and we also highlighted the two categories of threat, which basically include natural types of security threat and manmade types of security threat, but in the last unit, we only discussed major types of natural threat. As you may have been aware, natural threats are basically those threats created by nature, and there is little or nothing that man can do to prevent such threats from occurring within geophysical space. Notwithstanding, there are ways through which man can still manage those threats especially by creating viable framework for hazard mitigation, hazard assessment, among others.

On the other hand, there exist also threats emanating from actions and behaviour of man, which can undermine the security of any community. For instance, activities of terrorists might attract greater losses in human and material terms than any natural threat. The reason is that it is now found to be easier to manage all natural threats except earthquake that cannot be predicted than terrorism. The latest most grievous experience of using passenger aircrafts to cause a situation of mass destruction evident in the September 11, 2001 terrorist attack in the US re-echoes the monumental threat that acts of terrorism can constitute not only to countries but also to the world at large. In this unit, we shall be beaming our searchlight on various manmade security threats.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Identify major manmade types of security threat,

Discuss the meaning of the various manmade security threats; and

Explain their characteristics of these threats and how they constitute security risk to any community.

3.0 MAIN BODY

3.1 **Robbery**

One example of manmade threats is robbery, and robbery often involves the use of instruments of intimidation and coercion by a party(ies) against another party(ies) with the aim of compelling the victim party to concede his/her property in question to the offender party. Such violent instruments like gun, knife, sword, cutlass, grenade, or other dangerous objects as the case may be, are usually used by robbers to force victims to yield to their (robbers') demand.

Robbery is a regular feature of every human society, even among animals, robbery takes place. For instance, in some wildlife clips, we see some hyenas hunting preys and eventually succeeding in catching some of these preys like antelopes. But, shortly after the catch, a group of lions larger in number may emerge from nowhere chasing away the poor hyenas and rob them of their catches (animals killed by the hyenas for feeding). This example nevertheless shows that the incidence of robbery is not limited to human beings but also exists in the animal kingdom.

Robbery is the crime of seizing property through violence or intimidation. This is different from embezzlement, larceny, and theft. Piracy is a type of robbery. Armed robbery involves the use of a weapon. Highway robbery takes place outside and in a public place. Robbery is generally an urban crime. Carjacking is the act of robbing a car from a victim, usually at gunpoint (://www.knowledgerush.com/kr/encyclopedia/Robbery).

Robbery is taking or attempting to take something of value from another by violence or the threat of violence. Robbery can be committed against individuals, businesses, and institutions like banks. It is a felony in all states. Threatening people on the streets with a baseball bat and demanding all their money and jewelry is robbery, even if the person is not injured. Pushing an elderly woman down on the sidewalk to steal her purse is also robbery (://criminal-law.freeadvice.com/violent_crimes/offenses _ robbery.htm).

Types of robbery

a) Piracy: This is one of the types of robbery. But, we need to exercise some caution in the conceptualisation of the concept of piracy. This is because in intellectual property and copyrights law, the term piracy is also used to describe the nefarious activities of offenders who steal the works of other people especially for money-making motives. However, the piracy we are discussing in this study or lesson is essentially maritime. The term piracy is described in the relevant provisions of the United Nations Convention on the Law of the Sea (UNCLOS) of 1982 as:

(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
(i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
(ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
(c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b) (UNCLOS, 1982: Article 101).

Piracy usually involves a very violent act perpetrated by private parties of no government affiliation. Piracy is a violent crime and robbery that takes place on the seas. A good example includes the nefarious activities of Somalian criminals or pirates who rob and seize ships on the sea, a situation which has attracted so much public attention in recent times. Piracy is a form of robbery that involves all violent acts perpetrated on the seas but it does not include those criminal activities being perpetrated by passengers against some other passengers on the same vessel. The phenomenon of piracy is not new but has been an agelong security threat, which in the 17th and 18th centuries attracted death penalty against the offenders. During these periods in Europe, pirates caught and arrested were paraded before the public and later subjected to public execution;

b) Car-snatching or Carjacking: This is another type of robbery that has been phenomenal in a number of countries including South Africa, the US, Sweden, Nigeria, among others. It can be described as the act of forcefully seizing and taking possession of the victim's car by the crime offender with the use of dangerous weapons especially gun. We can also define this form of robbery as:

.....an armed auto theft, or auto theft by threat or force from a person (**Error! Hyperlink reference not valid.**).
.....the crime of motor vehicle theft from a person who is present. Typically the carjacker is armed, and the driver of the car is forced out of the car at gun point (://ww.knowledgerush.com/kr/encyclopedia/Carjacking).

In some situations, the car-snatcher may use a toy gun to force the victim (carry owner or driver) out the car. If the offender is arrested, he/she will still be liable to be charged for armed robbery because he/she, by using gun either toy or real, intends to cause fear or intimidation on the victim with the aim of criminally seizing and/ or stealing the car from the victim. In South Africa, the incidence of car snatching is very high, and in the process of stealing cars from victims, many victims have not only lost their cars but also their lives or lives of co-occupants (or loved ones) or sustained various degrees of injury in the hands of car-snatchers.

Car-snatching often generates trauma among the victims. For instance, some years ago, a popular reggae artist, Lucky Dube was killed by a gang of car-snatchers in South Africa in the presence of his child. Can you imagine the amount of trauma suffered by the child, seeing his father being hunted down by some criminals in the name of car-snatching? The Shina-Rambo episode in Nigeria is still very fresh in the memories of many of us who knew the amount of security threat the car-snatching syndicate posed to our national security. The leader of the syndicate, Amani Tijani has been arrested and as currently facing trial in Nigeria.

More importantly, one is expected to know that there is a difference between ordinary car theft and car-snatching. The truth of the matter is that not all incidents of car theft can be regarded as car-snatching or carjacking. This is because there may be occasions where cars are stolen from where they are parked. In this case, cars are stolen without forcefully taking them from the drivers. Here, the car thieves carefully remove and steal the cars from where they are parked or by deceiving the car drivers or owners. This kind of crime can only be regarded to as car theft and not car-snatching or carjacking;

c) Streaming: This is another type of robbery that usually involves organised criminal activities being perpetrated on underground trains. The term is made popular in the United Kingdom, and used to describe the violent crimes perpetrated on train or bus passengers by criminal gangs (see ://news.bbc.co.uk/1/hi/england/6983476.stm; & **Error! Hyperlink reference not valid.**). The crime ranges from mild application of intimidation and violence to the use of serious violence like rape, assault and murder;

d) Highway robbery: Highway robbery can also be regarded as a great threat to security. It can simply be described as a kind of robbery that takes place on the roads, streets, or even bridges. This threat is often experienced by many commuters using Nigerian roads. Meanwhile, there are some hotspots where the incidence of highway robbery frequently takes place. One of such spots is Abuja-Lokoja road where several passengers and travellers have been robbed or/and injured or/and killed by suspected highway robbers. A pathetic case was the incident of highway robbery that happened recently where many victim passengers were crushed to death by an on-coming trailer, which was on top speed while they were being pinned-down by the robbers. The ugly incident happened when the victim passengers were asked by the robbers to lie and face down, and many of the victims never suspected that the trailer approaching would crush them.

e) Armed robbery: This is another type of robbery, which involves the use of weapons. The weapons used by the robbers may not necessarily be deadly. Take for instance, a robber may be armed with table knife to dispossess his/her victims. Some robbers may use big sticks to force their victims to surrender their valuables. Some robbers may use their physical strength to dispossess their victims (especially the female) of their valuables. Such action may still be regarded as armed robbery; and

f) Aggravated robbery: Aggravated robbery actually means a form of robbery where the offenders use deadly or dangerous weapons in the course of carrying-out their dastardly act. Aggravated robbery can also be defined as:

> *....the use of a deadly weapon or what appears to be a deadly weapon. If someone robs a store with a toy pistol, that will still be aggravated robbery, because the weapon appeared to be deadly. It is also aggravated robbery in some states to cause or threaten serious bodily injury or death during the commission of the robbery* (://criminal-law.freeadvice.com/violent_ crimes/offenses_ robbery. htm).

The experience in recent time has shown the high level lethality in the weapons being used by some robbers in carrying out their dastardly acts. The incidents of bank robbery have taken very aggravated dimension where robbers don't only use sophisticated riffles but also use grenades. The warlike situation that characterises bank robbery in Nigeria in contemporary time underscores the need to appreciate security reengineering and reformulation of security strategies.

SELF ASSESSMENT EXERCISE

Explain the meaning of robbery

Discuss any five types of robbery

3.2 Theft

Theft can also be said to be a form of manmade security threat. It actually involves act of making unlawful claims over someone else's property or "illegal taking of another person's property without the person's freely-given consent" (://en.wikipedia.org/ wiki/Theft). Ordinarily, the term theft is used to describe some other criminal acts that relate to illegal acquisition of another person's property or acts of stealing like burglary, larceny, looting, fraud and embezzlement, to mention a few. Theft can be perpetrated in various ways. One of the ways may involve illegal access or intrusion into information systems belonging to another person or organisation.

The acts of theft are not exclusively undertaken by individuals because organisation(s) can also be found culpable. For instance, several organisations have been accused of stealing information belonging to some other organisations, either through the use of an insider or direct intrusion for the actualisation of specific objectives. Theft may also involve the unintentional stealing of another person's property. For instance, someone may accidentally find another person's unused (phone) recharge card, and rather than returning it, he/she may decide to sell or use it. In the situation whereby the person in question decides to sell or use the recharge card, he/she has committed theft, showing that it is not always necessary for the act of theft to be intentional. By and large, theft does not in any way involve the application of direct force against the victim, and in a situation where this happens, the act can no longer be regarded as theft, but will be considered a robbery.

SELF ASSESSMENT EXERCISE

Explain the meaning of theft as a threat to security.

3.3 **Arson**

Arson can be described to mean a deliberate act of destructively setting another person's or oneself's property on fire for specific motives. For instance, someone can decide to set his/her property on fire with the criminal intention of illegally getting claims from the insurance company. Most times this crime is usually perpetrated by one party against another party. The antagonistic and destructive politicking that dominates our national politics has paved the way for the growing anarchy that the country experiences.

From one democratic dispensation to another, the incidence of arson has been featuring not only in inter-party relations but also in intra-party wrangling. The use of thugs to set fire on the houses of opponents is still experienced in Nigerian politics. For instance, the last re-run government election in Ekiti State of Nigeria saw the burning down of the Independent National Electoral Commission (INEC) office in Ido Ekiti by irate youths over the alleged manipulation of election result by the election body and a few powerful people in the state. There is no doubt that, in the country, arson constitutes a great security threat especially if we consider the amount of material losses that usually occasion such incident(s).

SELF ASSESSMENT EXERCISE

What is arson?

3.4 **Kidnapping**

The incidence of kidnapping has become a grave security threat both locally and internationally. Many families have lost their loved ones through the dastardly acts of kidnapping. Apart from loss of lives, kidnapping also has implications on the economy of the state as well as that of individuals. For instance, in countries like

Mexico and Nigeria where most kidnappings lack political motives, the kidnappers seize their victims for ransoms, and many families pay through the nose to settle the kidnappers' money requests with the aim of securing the release of their loved ones. At this point, let us quickly look at some definitions of the term kidnapping.

However, kidnapping can be described as a form security threat that involves:

.....the taking away or asportation of a person against the person's will, usually to hold the person in false imprisonment, a confinement without legal authority. This may be done for ransom or in furtherance of another crime, or in connection with a child custody dispute (://en.wikipedia.org/wiki/Kidnapping).

……the taking away of a person against the person's will, usually to hold the person for ransom or in furtherance of another crime. In the terminology of the common law in many jurisdictions, the crime of kidnapping is labelled abduction when the victim is a woman (://www.knowledgerush.com/kr/encyclopedia/Kidnapping).

The nefarious activities of some of the militants in the Niger Delta region of Nigeria has actually made popular kidnapping as a source of making quick money. The problem is spreading fast to other regions of the country. There is increasing tension in the south-eastern Nigeria where the business of kidnapping is becoming widely accepted among the youths in the area. It is most pathetic that in some circumstances, some of the victims of kidnapping were part of the plot right from the outset. They planned the kidnapping episode with some other criminals to get money from their family members or/and relatives or/and friends. Many drivers have also been accused of masterminding the kidnapping of their bosses or members of their bosses' families. There is no doubt that the rising incidence of kidnapping is a major source of worry to the security sector, especially as security personnel are not left out of being targeted by kidnappers. For instance, some practitioners have at one time or the other become preys in the hands of kidnappers. Many of these security men and officers were not lucky as they were killed by the kidnappers.

SELF ASSESSMENT EXERCISE

What is kidnapping?

3.5 Badger Game

Badger Game is a form of security threat that can undermine the capacity of an individual to perform his/her duties effectively well. The risk created by this threat deepens the vulnerability of the affected individuals through set-ups from opponents. Here, the individual or security officer is coerced to compromise his/her position by playing on his/her intelligence or tricking him/her into an action that people might not expect of him/her. For instance, a very principled security chief may be trapped with a woman, and his conversations and sexual relations with the woman recorded by his enemies who set him up in the first instance. Consequently, his/her enemies will approach him/her and ask him/her to compromise his/her position or will be blackmailed. This scenario reemphasises the need for security practitioners to always be very careful in their relations with other people and to avoid engaging in any action that can tarnish their image and that of the office they hold or which can make them compromise their position.

SELF ASSESSMENT EXERCISE

How do you describe badger game?

3.6 Extortion

Extortion is another form of manmade security threat. It simply involves coercing a person to part with either money, property or services to the offender. On daily bases, Nigerians complain of extortion being suffered in the hands of security operatives especially the Police. Conceptually, extortion can be described as:

.....a criminal offence, which occurs when a person unlawfully obtains either money, property or services from a person, entity, or institution, through coercion (**Error! Hyperlink reference not valid.**).

……a criminal offense, which occurs when a person obtains money or other goods from another by threatening or inflicting harm to his person, reputation, or property (://www.knowledgerush.com/kr/encyclopedia/Extortion).

Extortion occurs not only in public places but also in private establishments. Many people in the course of seeking for job are mandated to pay money or render some services against their will before they can secure employment. Commuters always accuse the police of extortion on our roads and even in their stations despite the prevailing anti-corruption campaign in the country. Many customs officials have failed to do their jobs effectively well because of their culture of extortion. They are basically preoccupied with extorting the public, and in the process they often fail to perform their responsibilities. One of the consequences of this failure is circulation of proliferated weapons in the country, which come in through the borders.

The culture of extortion has continued to paint the security sector in Nigeria in bad light, as the most needed cooperation from the public in the effective management of security is visibly lacking. One of the reasons is the fear of being extorted by security operatives, even when they (the civilians) wish to offer or provide important information to the security personnel for crime prevention and mitigation. There are several allegations that some individuals, after offering vital security information to the police, were arrested and threatened with violence and prosecution, until the affected innocent civilians were forced to settle the extortionist security men/officers with varying amount of money. It is most disturbing to hear cases where some security personnel demand for sex from their female victims before they could be released from unlawful detention.

The writer can remember when in the company of a friend, being intercepted by an anti-robbery patrol team before 8pm when there was no case of curfew, and subsequently, the arrest was effected without any genuine reason. At the station, the patrol team had arrested, in similar circumstances, scores of innocent civilians and ordered everybody into the cell without any investigation. The next thing we heard was that we should beg those whose relatives had come to pay for their release, to assist us to get in touch with our relatives or friends to come and negotiate our own release as well. Within a short time of the arrest, some neighbours of mine who saw me and my friend being whisked away by the criminals in uniform came to the station to pay for my release but I refused to succumb, requesting to see the Divisional Police Officer (DPO) of that station.

Consequently, I stayed there till the next morning but not without being assaulted by one of the policemen on duty. One of the inmates appealed to me to give peace a chance by accepting the terms of release (paying illegal money as bail), and because so much pressure from my neighbours, I gave in. To my greatest surprise, one of the policemen told me that it was a nice decision, accepting the terms of my release. Money was forcefully taken by the police to secure my release and that of my friend. The policeman went further to say that if I had insisted to settle the case in court, he was very sure, due to lackadaisical and ineffective justice system in the country, that the court would ask us to be remanded in prison, even without making attempt to find out if the arrest was a lawful one in the first instance.

Sadly, the police that is supposed to be friendly to people and make efforts towards promoting developmental and democratic ethos has rather been an institution filled with agents of anarchy and exploitation (Alemika, 1993). Police men in Nigeria often use several forms of brutality with the aim of exploiting innocent civilians (Alemika 1999: 10). The experience of most civilians, resulting from unofficial extortion by security operatives in the country undermines the integrity and capacity of the public security sector to fulfill the overall goals of their establishment particularly the security of lives and property of the citizens.

SELF ASSESSMENT EXERCISE

Describe extortion as a security threat.

3.7 Insurgency

Insurgency is another form of manmade security threat. It usually involves an armed struggle or rebellion aimed to challenge the sovereign power of a constituted authority. It can also be described as violent aggression by belligerents against the government of any given country, especially the one recognised by the United Nations (see Oxford English Dictionary, 1989). However, we can also define insurgency as:

...an organized rebellion aimed at overthrowing a constituted government through the use of subversion and armed conflict (://wordnetweb.princeton.edu/perl/webwn).

...an armed uprising, revolt, or insurrection against an established civil or political authority. Persons engaging in insurgency are called insurgents, and typically engage in regular or guerrilla combat against the armed forces of the established regime, or conduct sabotage and harassment in the land (://www.answerbag.com/q_view/68079).

Some of the causes of insurgency may include electoral malpractices as experienced in Algeria, ethno-religious conflict, human rights abuse, personal envy, maladministration, ineffective justice system, to mention a few. The problem of insurgency has been a regular feature of African politics due to a number of reasons. One of the reasons is the sharp ethnic division that exists among various ethnic groups, which compose average African state. This problem is prevalent where there is deepened economic deprivation and patron-client network. In such a country, the elite are often accused of flying the kite of ethnicity in the accumulation of state resources thereby creating a culture of ethnic hatred as evident in Rwandan crisis.

The ideological rivalry between the Angolan government and the National Union for the Total Liberation of Angola (UNITA) rebel led by late J. Savimbi especially during the cold war era has also shown how ideological differences can attract insurgency in any given state. There is no doubt that most insurgent groups use the instrument and tactic of terror to attract public attention to themselves. And most times, methods applied by insurgents do not only undermine the security of lives and property, but they also infringe on the natural rights of the innocent civilians and dislocate them socially and economically.

SELF ASSESSMENT EXERCISE

How do you explain insurgency as a security threat?

3.8 Terrorism

Terrorism of course, is not a modern concept. The term terrorism trod its semantic pathway to the English usage in 1795. The term was popularized by the Jacobins who ruled France between 1793 and 1794, as their reign was labelled as a reign of terror. Right from 1798, the word terrorism has become a regular vocabulary to explain the attempt by some individuals, state actors or groups to articulate their political goals and aspirations through the application of systemic violence.

What is terrorism? In the definition of terrorism as a concept, Wilkinson observes the underlying problems or dilemma, which detonate the subjective nature of terror

(Wilkinson, 1977) because it appears to be a "complex interplay of the subjective forces and …frequently irrational individual responses" (Wardlaw, 1989: 8), making the definition of terrorism a difficult one. Bruce Hoffman contends that:

> *On one point, at least, everyone agrees: terrorism is a pejorative term. It is a word with intrinsically negative connotations that is generally applied to one's enemies and opponents, or to those with whom one disagrees and would otherwise prefer to ignore. 'What is called terrorism,' Brian Jenkins has written, `'thus seems to depend on one's point of view. Use of the term implies a moral judgment; and if one party can successfully attach the label terrorist to its opponent, then it has indirectly persuaded others to adopt its moral viewpoint.' Hence the decision to call someone or label some organization `terrorist' becomes almost unavoidably subjective, depending largely on whether one sympathizes with or opposes the person/group/cause concerned. If one identifies with the victim of the violence, for example, then the act is terrorism. If, however, one identifies with the perpetrator, the violent act is regarded in a more sympathetic, if not positive (or, at the worst, an ambivalent) light; and it is not terrorism* (Hoffman, 1998: 32).

Terrorism is undoubtedly the systematic and ferocious use of violence, a form of guerrilla alternative to conventional warfare by state or non-state actors, with the strategic creation of psychic fear and (or) tactical production and reproduction of wanton destruction in epochal dimension purposely in realizing political objectives or ordinary public attention or both variables. There are different forms of terrorism. According to the United States' National Advisory Committee on Criminal Justice Standards and Goals, various forms of terrorism can be summarised as follows:

- ***Civil Disorders*** *– A form of collective violence interfering with the peace, security, and normal functioning of the community;*

- ***Political Terrorism*** *– Violent criminal behaviour designed primarily to generate fear in the community, or substantial segment of it, for political purposes;*

- ***Non-Political Terrorism*** *– Terrorism that is not aimed at political purposes but which exhibits "conscious design to create and maintain high degree of fear for coercive purposes, but the end is individual or collective gain rather than the achievement of a political objective";*

- ***Quasi-Terrorism*** *– The activities incidental to the commission of crimes of violence that are similar in form and method to genuine terrorism but which nevertheless lack its essential ingredient. It is not the main purpose of the quasi-terrorists to induce terror in the immediate victim as in the case of genuine terrorism, but the quasi-terrorist uses the modalities and techniques of the genuine terrorist and produces similar consequences and reaction. For example, the fleeing felon who takes hostages is a quasi-terrorist, whose* *methods are similar to those of the genuine terrorist but whose purposes are quite different;*

- ***Limited Political Terrorism** – Genuine political terrorism is characterized by a revolutionary approach; limited political terrorism refers to "acts of terrorism which are committed for ideological or political motives but which are not part of a concerted campaign to capture control of the State; and*

- ***Official or State Terrorism** –"referring to nations whose rule is based upon fear and oppression that reach similar to terrorism or such proportions." It may also be referred to as* **Structural Terrorism** *defined broadly as terrorist acts carried out by governments in pursuit of political objectives, often as part of their foreign policy* (National Advisory Committee on Criminal Justice Standards and Goals, 1976).

Proliferation of weapons and technological advancement brought to fore by the cold war as well as cacophonic international media coverage of international terrorism had really altered the traditional philosophy of terrorism. Mass destruction has become an object of international recognition and yardstick to measure the success of any terrorist network or group, a situation that has mounted a great challenge to security practitioners worldwide. And it is very important for the security sector to develop alternative strategies and reforms that will reduce the vulnerability of the existing system to any form of threat either natural or manmade.

SELF ASSESSMENT EXERCISE

Briefly discuss terrorism as a form of security threat.

3.9 Ethno-Religious Conflict

Ethnic origin or affiliation and religion have become fundamental elements of post colonial Nigeria. They hinge on ideology of excluvicism and primordial affections. Enemy imaging that characterises ethno-religious relations in Nigeria has continued to pose a huge security risk to the country. In the last, ten years, several thousands of people have either been killed, injured or/and internally displaced. Apart from deaths, various degrees of injury, and internally displacement of persons that are usually featured in ethno-religious riots in the country, there is also massive destruction of properties. In Africa, inter-ethnic rivalry has continued to constitute a huge security threat to the people as many countries on the continent have experienced civil war at one or the other due to rising ethnic nationalism and inter-ethnic hatred (Kasali, 2009: 72-72). The examples include Nigeria (south-eastern people of Nigeria or Biafra vs. The rest of Nigeria), Liberia (Putu vs. Krio), Mozambique (Shona vs. Ndebele), Rwanda (Hutu vs. Tutsi) etc. The

In Nigeria, ethno-religious conflict is the highest contributor of underdevelopment as ethno-religious riots have claimed many physical structures and infrastructure that took the affected communities several decades to develop. This phenomenon has nevertheless undermined the economies and investment-driving profiles of the affected communities, as many local and foreign investors fear to invest in those turbulent areas because of the risk that ethno-religious riots might pose not only to their businesses but also their lives and those of their employees, undermining the economic security of the affected communities in particular and the country in general.

The inept handling of ethno-religious and other forms of riot by Nigerian Police has been a source of worry as it is most times takes intervention of the military before normalcy is restored. Law enforcement agents have also been accused of exhibiting ethno-religious sentiments in the discharge of their duties. For instance, Onyeozili (2005) claims that police in Nigeria have bad image for taking sides in handling ethnic or communal riots, and often escalating the conflicts. He alleged that Nigeria police "brazenly participated in flushing out south-easterners from hiding during the military pogrom and the 1966 massacre of Easterners in the north" (Onyeozili, 2005: 41). If the argument of Onyeozili (2005) is right, the issue of ethno-religious conflict is reaching an alarming dimension because it will be more destructive if the Police or any other law enforcement agents that are supposed to quell ethno-religious riots are also found displaying ethno-religious sentiment or intolerance in the discharge of their functions.

SELF ASSESSMENT EXERCISE

Explain ethno-religious conflict as a manmade security threat.

4.0 CONCLUSION

In the last units, we have studied the meaning and basic categories of security threat. The growing danger that many manmade threats pose to the survival of any community has actually attracted increasing attention of various security stakeholders and practitioners to fathom ways, through which the impact of the manmade security threats can be reduced or prevented. The advancement in world technology has further made the world unsafe and on the verge of perpetual fear particularly resulting from the development of nuclear weapons and other lethal substances that can decimate the population by more than 25% if they are used. In the event of the usage of nuclear weapon by any state or non-state actors, no less than 2.5 billion people will be affected directly or indirectly. Also, the ecosystem will not be spared by the very destructive effect that nuclear weapon can pose to the planet. It is against this background that many national governments and non-governmental organizations (NGOs) through bilateral or multilateral arrangements to discourage proliferation of weapons or the use of deadly weapons through several treaties and agreements like Strategic Arms Limitation Treaty (SALT I & II).

5.0 SUMMARY

In this unit, we began our search into various manmade security threats by describing the meaning and types of robbery. Thereafter, we discussed some other types of manmade security threats including theft, arson, kidnapping, badger game, extortion, insurgency, terrorism and finally ethno-religious conflict. You are expected to note that there are several other types of manmade security threat that we could not treat in this study due to limited time and space. And some of these threats include corruption and embezzlement, gender discrimination, ethnocentrism, to mention a few. You are, therefore, admonished to always engage yourself in further reading because it is difficult to have an instructional material that will cover all areas of discourse pertaining to any course. By and large, we hope that you have found this unit very interesting. But, subsequently, we shall explore some other security threats yet to be discussed in the last units.

6.0 TUTORED MARKED ASSIGNMENT

Discuss any five types of manmade security threat.

7.0 REFERENCES AND FURTHER READING

Alemika, E. E. O. (1993). Colonialism, State and Policing in Nigeria. *Crime, Law and Social Change* 20: 189-219.

Alemika, E. E. O. (1999). “Police Community Relations in Nigeria: What Went Wrong?” Paper Presented at the Seminar on Role and Function of the Police in a Post-Military Era, Organized by the Centre for Law Enforcement Education in Nigeria (CLEEN), and the National Human Rights Commission (NHRC) at the Savannah Suite, Abuja, F. C. T., from 8th to 10th March.

Hoffman, B. (1998). *Inside Terrorism*. New York: Columbia University Press.

Kasali, M. A (2009). *PCR 261: Culture, Values and Conflicts in War*. National Open University of Nigeria.

National Advisory Committee on Criminal Justice Standards and Goals (1976). *Disorders and Terrorism.* Washington D.C.

Oxford English Dictionary (1989). Second edition.

United Nations Convention on the Law of the Sea (UNCLOS) of 10 December 1982, Part VII: High Seas, Article 101. Also available on ://www.un.org/Depts/los/convention_agreements/texts/unclos/part7.htm. Retrieved on 4 September, 2009.

Wardlaw, G. (1989). *Political Terrorism: Theory, Tactics and Counter Measures*. Cambridge: Cambridge University Press (2nd Edition).

Wilkinson, P. (1977). *Terrorism and the Liberal State*. London: Macmillan.

://criminal-law.freeadvice.com/violent_crimes/offenses _ robbery.htm. Retrieved on 31 August, 2009.

Error! Hyperlink reference not valid.. Retrieved on 31 August, 2009.

://en.wikipedia.org/wiki/Kidnapping. Retrieved on 30 August, 2009.

://en.wikipedia.org/wiki/Robbery. Retrieved on 31 August, 2009.

://en.wikipedia.org/ wiki/Theft. Retrieved on 31 August, 2009.

://news.bbc.co.uk/1/hi/england/698 3476.stm. *Retrieved on 3 September, 2009.*

://wordnetweb.princeton.edu/perl/webwn. Retrieved on 31 August, 2009.

://www.answerbag.com/q_view/68 079. Retrieved on 1 September, 2009.

://www.btp.presscentre.com/Content/Detail.asp?ReleaseID=675&NewsAreaID=2. Retrieved on 4 September, 2009.

Error! Hyperlink reference not valid.. Retrieved on 3 September, 2009.

://ww.knowledgerush.com/kr/encyclopedia/Carjacking. Retrieved on 3 September, 2009.

://www.knowledgerush.com/kr/encyclopedia/Extortion. Retrieved on 3 September, 2009.

://www.knowledgerush.com/kr/encyclopedia/Kidnapping. Retrieved on 4 Sept., 2009.

://www.knowledgerush.com/kr/encyclopedia/Robbery. Retrieved on 3 September, 2009.

UNIT 3

INFORMATION WARFARE AS A SECURITY THREAT

CONTENTS

1.0 INTRODUCTION

Information warfare is a relatively new term that has become a popular vocabulary in national and international security settings. The concept of Information has traditionally been a prominent feature of warfare, even right from the primitive age. The concept has moved beyond the traditional methods of propaganda and spying.

Computers have brought a new dimension to information warfare. In contemporary time, computers are used to perform a lot of functions as they now have great impact on every aspect of human relations and development. Ten years ago, no less than 400 million people were using computers for various tasks but now the there are more than 1 billion computer users, which shows the growing relevance computers enjoy in the new world order.

Well, the basis of this unit is not only to conceptually define information warfare but also to focus on how information technology constitutes a security threat. It will amount to disservice, if we fail to explain some of the major types of (modern) information warfare. This we shall avoid by drawing our search-light also on various types of information warfare. Thank you in anticipation for your attention. It is my belief that you will find this unit very interesting.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Define information warfare;

Discuss how it constitute a security threat; and

Identify types of information warfare

3.0 MAIN BODY

3.1 **Describing Information Warfare**

Traditionally, parties sought to know the strategic secrets of the other parties with the aim of gaining strategic advantage over the enemy parties. Some people would be sent to enemies’ camps for information-sipping and espionage. Information could also be applied in form of propaganda and destructive rumours with the aim of subjecting the enemy-party to perpetual confusion for political reasons.

Presently, information has assumed a more prominent role in relation between one actor and the other in contemporary global system. The reason for this is not far-fetched. The emergence of information revolution has created a new expression and a paradigm shift in modern warfare (Libicki, 1995).

The philosophical idea, which formed the basis of the emerging information warfare can be ascribed, or better still be linked to Sun Tzu ideological orientation, which is interpreted as thus:

(A)ttaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence (Translated in Sawyer, 1994).

Sun Tzu tried to present another face of strategy and warfare when he stressed on the importance of creative application of information among parties, the greatest strategy through which parties can meet their political goals rather than adopting the traditional means of warfare like the use of weapons. The use of information in warfare is relatively cheaper but its implication may be unprecedented and more destructive than the traditional means of warfare.

Let us consider a scenario whereby young children arching information from a nation's military intelligence network, and subsequently corrupt and destroy its strategic information infrastructure. Consequently, the impact of such electronic intrusion and damage may be more devastating than aerial bombardment of such nation. This tells us the importance of information technology in modern warfare and security management.

The definition of information warfare has been a great subject of debate, especially in the 1990s. The term information warfare appears too wide. It includes several aspects of traditional military policy such as battlefield command and control warfare (C2W) as well as other traditional types of electronic warfare (EW). Then, what is information warfare? According to the Institute for the Advanced Study of Information Warfare:

Information warfare is the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information systems, while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries (.psycom.net/iwar.1.html).

The International Centre for Security Analysis describes information warfare as "struggles for control over information activities". It goes further to identify and analyse various categories of information warfare, according to her: the first category "encompasses the whole range of psychological, media, diplomatic and military techniques for influencing the mind of an opponent, whether that opponent is military commander or a whole population".

In addition, the second category will focus on the ways through which the military or the security sector can be transformed to the one that can dominate the "information spectrum". Thus, information dominance can be achieved through a party engaging the other (enemy party) in a physical conflict "either unnecessary or at worst short, sharp and successful". The last category involves any form of electronic assault directed against either the military or civilian information facilities (or both) of the enemy party.

According to the US Air Force, information warfare can be described as:

(a)ny action to deny, exploit, corrupt, or destroy the enemy's information and its function-while protecting ourselves against similar actions (US Air Force (1995, 3-4)

Mark Jacobson on his part, defines information warfare as:

(a)ctions taken to preserve the integrity of one's information infrastructure from exploitation, corruption(,) or destruction while at the same time exploiting(,) corrupting (,) or destroying an adversary's information systems (,) thereby achieving a military advantage (see .infowar.com/resource/warfare.doc).

The French Ministry of Defence describes information warfare as a concept, which exhibits itself in three basic forms. And these forms help us in the conceptualization of the term information warfare. According to her, the elements of information warfare include:

War for information (guerre pour l'information): to obtain information about the enemy's means, capabilities and strategies in order to defend ourselves;

War against information (guerre contre l'information): at the same time to protect our information systems and disrupt or destroy the enemy's;

War through information (guerre par l'information): to conduct misinformation or deception operations against the enemy in order to achieve "information dominance" (see Moliner, 1998: 11).

Information warfare involves the application of computer and its related mechanisms basically to plunder the military and/or civilian information networks of the enemy party. It is no gainsaying that information warfare has begun to receive growing interest among scholars in the field of security studies and policy makers due to its ability to destroying military powers of enemy party.

However, information warfare is not prosecuted like traditional warfare. It is often waged through disabling and crashing "an enemy's armed forces and civilian infrastructure without the use of a single bullet. The computer is the weapon of the twenty-first century" (see .bu.edu/law/scitech/volume6/Robbat.htm#ftn1).

Information has remained a veritable tool of warfare from time immemorial. But it has assumed a new dimension since the emergence of information revolution resulting from the rapid sophistication of modern technology. The trend of modern information system has made war a very interesting discourse.

Meanwhile, how will you feel, having a situation where nations or individuals conduct war more through application of (modern) information systems rather than the traditional physical aggression? What damage can a super-power like the US suffer that is greater than crushing its economic power or hegemony?

Through information sipping, Asian countries like China have continued to constitute an enormous threat to the US by imitating (or thieving) the American technology models especially in automobile industry. The US would manufacture a car model while China will do its imitation with improved quality, may even sell it at cheaper rate, forcing buyers including Americans to rush for the China products. Due to the emergent information revolution that characterizes the relations among state and non-state actors, it is no news that war is fought on a daily basis through information, and nonetheless:

There are countless ways malicious people can use a computer to perform illegal activity—hacking into systems, leaking trade secrets, unleashing new viruses, using phishing messages to steal personal information, and so on. And we are constantly hearing about new exploits (://www.microsoft.com/technet/technetmag/issues /2007/12/Forensics/).

The growing relevance of computers has nonetheless culminated in the contemporary security threat that we face at every level of human relation, from personal through national to global affairs. Enemy parties now give priority attention to ways they can have strategic advantage over one another by attacking one another’s information systems. These attacks are capable of not only destroying the information systems but also constituting a threat to military and civilian infrastructures (see Lyett & Ibrügger, 1997).

SELF ASSESSMENT EXERCISE

What is information warfare?

3.2 Types of information Warfare

a) Data Attacks: These are done by inserting data into an information system to distort its functionality like application of computer virus. The computer viruses are often small programmes created and developed by some computer science students, hackers, despicable programmers and some nefarious computer corporations. These viruses are very destructive as they can easily corrupt the information files on the target system(s), make the system(s) malfunction or even crash the disk operating system (DOS) or even the storage facilities like the hard drive;

b) Software Attacks: These involve penetrating the target information system(s) by applying software to steal information or make the system(s) to fail, malfunction or crash. There are software packages that can enable one's password to be accessed illegally while there are some others, which can make the systems to malfunction. Some software if applied on your system will look for some specific security files automatically allowing hackers to sip information from your system(s) or even electronically destroy it;

c) Hacking and Cracking: This involves illegitimate entry into or control of information system(s) to steal information or cause some forms of damage or destruction to the system(s) including deleting of the target information (files). Many of these hackers usually have evil intentions. They sometimes attack their victims' systems to destroy them completely or to spy and/or steal vital information from the systems.

For instance, in the United States within the period of almost eleven months (January to mid November 1998), the National Security Agency (NSA) revealed that no less than 3800 illegal intrusions were attempted by hackers against the Defence Department's unclassified computer systems and networks. But there's the likelihood or possibility that the NSA deliberately reduced the actual number of the intrusions for strategic reason(s). This is because there are speculations that the actual number of intrusions was higher than the figure announced or made public by the NSA (.wired.com/news).

Another example is the case of two British boys who hacked or gained illegal access into the system of the Air Force's laboratories in New-York. The boys gained the intrusion through the use of "sniffer" programme, which allowed them to get the passwords and user-log-ins to the system network (see .iwar.org.uk/iwar/resources/nato/as285stc-e.html).

It was no surprise, that in an attempt by the US to contain the security threat being posed by the activities of hackers to its national security especially the defence, the government allowed Pentagon to conduct a simulation exercise in the summer of 1997. The simulation exercise was tagged "Eligible Receiver". The reason for the exercise was to see how much the US military and civilian infrastructure could resist intrusion(s) and attack(s).

Therefore, a group of hackers known as the Red team was set up to do the intrusion test. Though, the result of the exercise was not made public by the government, James Adams, a Washington based journalist revealed, after conducting a number of (secret) interviews for several senior officials of the Pentagon that:

> *The [simulated] attacks focused on three main areas: the national information infrastructure, the military leadership and the political leadership. In each of these three areas, the hackers found it exceptionally easy to penetrate apparently well-defended systems. Air traffic control systems were taken down, power grids made to fail, oil refineries stopped pumping* - *all initially apparent incidents. At the same time, in response to a hypothetical international crisis, the Defence department was moving to deploy forces overseas and the logistics network was swinging into action. It proved remarkably easy to disrupt that network by changing orders [Š] and interrupt[ing] the logistics flow [Š]. The hackers began to feed false news reports into the decision-making process so that the politicians faced a lack of public will about prosecuting a potential conflict and lacked detailed and accurate information [Š]* (quoted in Walker & Fidler, 1999).

There is no doubt that the danger posed by hacking to private and public security is enormous. In the United States, the Federal Bureau for Investigation (FBI) once reported saying that almost $10 billion is lost in the US through the nefarious activities of the hackers (ibid). Such amount of money is far greater than the annual budgets of several countries in Africa and elsewhere; and

d) <u>Physical Attacks</u>: This usually involves the use of traditional techniques like physical destruction of information system through arson, bombing or hitting an object against the system with the intention of destroying it. According to North Atlantic Treaty Organization (NATO) Draft Report on information warfare and international security:

> *The immediate energy release from the denoted nuclear device produces intense, rapidly varying electric and magnetic fields that can extend for considerable distances and severely affect all electronic equipment and electrical or radar even to the point of destroying equipment circuits, microprocessors, and other component. Therefore, a single, very high altitude nuclear blast….which may cause no physical damage to structures or people, could disable all non-hardened information systems* (see **Error! Hyperlink reference not valid.**).

Considering the foregoing, you may agree with me that a physical attack can be targeted against information system(s) through the use of several means particularly the electro-magnetic pulse (EMP), which can be produced by nuclear explosions.

SELF ASSESSMENT EXERCISE

Discuss types of information warfare

4.0 CONCLUSION

There is rapid increase in people's and nations' reliance on computers. This is due to the great impact information has on human and capital development. The growing relevance of computers has also constituted a security risk to the world at large. There is no doubt that the emergent information revolution will have some great impact in conventional military engagement. It is no news that war planes are now being equipped with more precision gadgets that will make it possible to hit the targets with little or no civilian causalities. Information revolution has also made it possible to 'crash' a plane without shooting but through information manoeuvre.

5.0 SUMMARY

In the unit, we have been able to define the term information warfare and explain how information warfare constitutes a security threat not only to nations but also individuals as well as corporate entities. We thereafter discussed some of the basic types of information warfare, which may include data attacks, software attacks, etc.

6.0 TUTORED MARKED ASSIGNMENT

Define the meaning of information warfare and explain four types of information warfare.

7.0 REFERENCES AND FURTHER READING

Adams, J.(1998). *The Next World War*. London: Hutchinson.

Libicki, M. (1995). *What is Information Warfare?* Washington, D.C.: Centre for Advanced Concepts and Technology/National Defence University.

Lyell, L. & Ibrügger, L. (1997). *Information Warfare and the Millennium Bomb*. General Report, NAA Science and Technology Committee [AP 237 STC (97) 7]. Also available on ://www.iwar.org.uk/iwar/resources/nato/as285stc-e.html- 2. Retrieved on 6 January, 2008.

Molander, R. C., Riddile, A. S. & Wilson, P. (1996). *Strategic Information Warfare: A New Face of War*. Santa Monica, California: RAND, MR-661-OSD.

Moliner, J. (Colonel) (1998). La Guerre de L'information Vue Par Un Operationnel Francais. *L'Armement*, No. 60, Decemeber 1997-January 1998. Translated on .iwar.org.uk/iwar/resources/nato/as285stc-e.html. Retrieved on 4 January, 2008.

Rathmell, A. (1998). Information Warfare and Sub-State Actors. *Information, Communication & Society*, Winter 1(4): 488-503.

Smith, George (1998), "An Electronic Pearl Harbour? Not Likely", *Issues in Science and Technology*, Fall.

Walker, Tony and Stephen Fidler (1999), "China studies Computer Warfare", *Financial Times*, 16 March.

://www.abcnews.go.com/. Retrieved on 20 January, 2008.

://www.iwar.org.uk/iwar/resources/nato/as285stc-e.html-14. Retrieved on 20 January, 2008

.bu.edu/law/scitech/volume6/Robbat.htm#ftn1). Retrieved on 20th January, 2008.

.infowar.com/resource/warfare.doc). Retrieved on 21st January, 2008.

.iwar.org.uk/iwar/resources/nato/as285stc-e.html). Retrieved on 21 January, 2008.

://www.microsoft.com/technet/technetmag/issues/2007/12/Forensics/. Retrieved on 18 January, 2008.

://www.mod.uk/policy/sdr/. Retrieved on 28 January, 2008.

.psycom.net/iwar.1.html. Retrieved on 28 January, 2008.

.wired.com/news. Retrieved on 28 January, 2008.

UNIT 4

ARMS PRODUCTION AND PROLIFERATION AS A POTENTIAL THREAT TO SECURITY

CONTENTS

6.0 Tutored Marked Assignment
7.0 References/Further Readings

1.0 INTRODUCTION

The issue of arms production and proliferation has been a source of worry in recent time. There is no doubt that the two World Wars have created an atmosphere of tension by laying solid foundation for arms race and pervasive insecurity. The incident of World War II has had some destructive effects on mankind as well as the general ecosystem without any limit in geographical boundary. The world has been greeted with proliferation of a variety of assaulted weapons and agents of mass destruction, where mutual deterrence has taken the form of Mutual Assured Destruction (MAD). The war has marked a new phase in the history of human tragedy. In 1945, America infested two Japanese cities of Hiroshima and Nagasaki with pestilence through the use of atomic bombs, which killed tens of thousands of people and many became deformed. Today, after 64 years of the US bombardment of these two Japanese cities, the local people as well as the ecosystem still suffer the effects of devastating damage caused by those military actions. In this unit, we shall study how arms production and proliferation constitutes a great threat to national and international security.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Explain the meaning of arms proliferation and production;

Discuss the origin of the current proliferation of weapons in the contemporary global system; and

Examine the threat constituted by arms distribution patterns to national and international security.

3.0 MAIN BODY

3.1 **Arms Production and Proliferation**

Arms proliferation may be defined as the spread of small arms or weapons designed for use by individuals like pistols, assault rifles, sub-machine guns and light machine guns. It may also involve spreading of light weapons which can be deployed and used by a group of two or more people, and these include grenade launchers, portable anti-aircraft and anti-tank guns, as well as recoilless riffles or even missile launchers and mortars (less than 100mm). It may also involve the spread of atomic bombs and other weapons of mass destruction, be it nuclear, biological or chemical, among the state and non state actors, particularly the criminal mass of people and rogue states (Treverton & Bennett 1997:1). However, except from the world powers, other state and non-state actors are not allowed to produce or be in possession of weapons considered as weapons of mass destruction.

On the production of small arms, depending on its sophistication, it can be produced anywhere in the world. In Nigeria, there are many outlets thriving in the production and sales of '*aba*' guns in the eastern part of the country. Guns and petrol bombs are manufactured in virtually all parts of Nigeria. But these local arms are crude and not sophisticated like the ones coming from Europe, America and Asia. One cannot compare '*aba*' riffles with the AK-47 assault riffles.

It is worth-knowing that, despite the sophistication of these rifles, they are cheap, robust and durable as they are very easy to manufacture. They can even be easily assembled, transported and used by children. For instance, in Liberian war, child-soldiers used AK-47 riffles in the prosecution of the civil war. This has given the international community a great concern to formulating and implementing strategic policy actions to reduce the proliferation level of small arms and light weapons particularly among the world civilian population. Thus, these weapons have continued to kill or exterminate an average of 200,000 people on annual basis in the so called peaceful societies, while over 300,000 people are killed in conflict ridden societies, as millions of people suffer various degrees of injuries (DFID, 2003:2).

Historically, during the Potsdam Conference (July 24, 1945) Josef Stalin of the Old Soviet Union was informed by the US President Truman on the intention of his administration to attack Japan, unless it (Japan) surrendered, with a very destructive bomb that had been developed by the US. This bomb would have much devastating and catastrophic effects on human and material resources. That bomb was atomic bomb! Student, it is better, we discuss briefly the history of the atomic bomb, to aid your understanding of the subject matter. In 1939, Albert Einstein wrote a letter to the then American President, Mr. Roosevelt, informing the President of the need to carry out a project on the development of atomic bomb and its possibility. This letter gave birth to the American Manhattan Project in September 1942. But prior to that, a Soviet Scientist, Georgi N. Flerov wrote the Soviet State Defense Committee in June, 1942 on the need to produce a uranium bomb. This period marked the beginning of arms race in modern history. Thus, according to C.M. Roberts:

On December 2, 1942, the first chain reaction was achieved at the University of Chicago. The comparable Soviet achievement came on December 24 1946. The Soviet Union did not produce sufficient plutonium for a nuclear bomb test until 1949, more than four years after the American test at Alamagordo, New Mexico (Roberts, 1974: 6).

After the innovation of the US in the development of Atomic bomb, the government of Soviet Union reacted swiftly by calling on its scientists and engineers to defend their homeland by building atomic bomb in no time. The reaction of the USSR government was to check the US monopoly of Atomic weapon or military supremacy, particularly when there was already a Cold War existing between the West and East divides. Again, after Soviet Union’s invention of atomic bomb, a series of cautions were made between the US and USSR because of their equal power relations to mutual destruction.

Five months after the first Soviet nuclear test, the US President Truman announced the intention of America to develop hydrogen bomb, a quantum jump in explosive power with the aim of maintaining arms superiority. By November 1, 1952, the H-bomb (Hydrogen bomb) was experimentally achieved in the US after the August 12 Soviet invention. This period attracted affection for Missile Artistry by the then two super powers (the US and USSR). By 1955, the two super powers had achieved deliverable H-bomb capabilities, but were striving vigorously to achieve Inter-Continental Ballistic Missile (ICBM) capabilities. The US later launched its first nuclear powered submarine and development of huge B-52 bombers. On 26 of August, 1957, the Soviet government announced the first test of an ICBM (Inter Continental Ballistic Missile) and six weeks later, she also announced the “Sputnik project”. Other ballistic missiles already developed were intermediate and medium range ballistic missiles (IRBMs and MRBMs).

The two super powers later developed (ABM) Anti Ballistic Missiles which the Soviet developed to provide limited defense against American Minuteman Missiles. The US developed ABM system before the Soviet Union. She (the US) first began with Nike-Zeus and then developed the then more advanced Nike X. Also in the 1960s, the US developed MRV (Multiple Warhead Re-Entry Vehicle), which carried a cluster of warheads for a buckshot effect. The US also considered in quick succession, the building on the Multiple Independently Guided Warhead Re-Entry Vehicle (MIRV). In Texas meeting, the US also considered the development of “poseidon”, a new MIRV missile for Polaris submarines.

In order to further check the American supremacy in strategic military build-up, the Soviet built new ICBMs, particularly the massive SS-9s as well as many nuclear powered ballistic-missile submarines often known as Yankee Class (Y-Class), which could match American Polaris Submarines. The Soviet also developed surface-to-air missiles (SAM). China and some other countries have joined the world nuclear powers, and there is an ongoing debate on the development of nuclear energy by Iran, which most western nations believe that it would spell a bad omen to the majority of the world population, if the US-coined “member of Axis of Evil” was developed by Iran.

One of the reasons is that Iran may supply some of the terrorist organizations in the world some of these destructive weapons to carry out their rebellious and destructive operations against their target state and non-state actors. There is a ban on the development of some weapons which, may be categorized as weapons of mass destruction by the world body and United Nations but notwithstanding, some super powers enjoy the production of these weapons.

Apart from these weapons of mass destruction like chemical and biological weapons among others, the world still looms with heightened insecurity and tension due to the proliferation of small arms and light weapons. Agents of destruction have increased world’s incident of terrorism, crime, human abuse and bloody conflict, promoting the attitude of intolerance and enmity and behaviour of violent revenge in the context of elongation of violent conflict and disorder. The genesis of this problem could be traced to the cold war era, which attracted military industrial complex initiative with attendant turmoil on humanity and disarticulation of spirit of friendship. The growing production of arms and weapons has been undermining the capacity of the security sector to guarantee the safety of lives and property. This also instructs the submission made by the erstwhile Secretary General of the United Nations, Mr Kofi Annan, and according to him:

Small arms proliferation is not merely a security issue; it is also an issue of human rights and of development (see the UN Millennium Report, 2000: 52).

In the 1990s alone, the number of small arms and light weapons in circulation was more than 200 million but now the figure has drastically increased due to bloody conflicts, civil wars and terrorist activities that have pervaded the entire globe. The current estimate of arms in circulation stands at no less than 500 million. This view is corroborated by Worldwatch Institute, stressing that:

More than 500 million military style hand-held weapons exist now- enough to arm every 12th human on earth - and millions more are produced each year, reports a new Worldwatch study released today. Violence fed by the uncontrolled spread of these weapons is further destabilizing societies already ravaged by war, poverty, and environmental degradation (Worldwatch Institute, 1997).

There is a growing number of illegal arms and weapons circulated among civilians in Nigeria. The incidence of violent crime has reached a very destructive dimension such that every innocent civilian and security practitioners in the country live in perpetual fear due to lethality in the weapons being used by criminal gangs in recent time.

3.2 **Arms Distribution Pattern: A Threat to Security**

Proliferation of arms or weapons has really posed a great challenge to the maintenance of law and order in all countries as no country can boast to be 100% free of violent crimes. The adverse effect of this threat to national and international security has necessitated giving greater security priority by various governments, initiating unilateral, bilateral and multilateral approaches and policies to limit the production of weapons particularly those considered capable of causing mass destruction like gas bomb. The world government has embarked on integration of defense, development, foreign policy, legal instruments and multilateral trade arrangement to mitigate the threat of arms/weapons production and proliferation. The world has become aware of the implications that arms proliferation can have on the world population, particularly those from post conflict societies and economically weak states like Nigeria. According to the Nairobi Declaration:

The problem of the proliferation of illicit small arms and light weapons in the region has been exacerbated by internal political strife and extreme poverty… a comprehensive strategy to arrest and deal with the problem must include putting in place structures and processes to promote democracy, the observance of human right, the rule of law and good governance as well as economic recovery and growth (The Nairobi Declaration, March 2000).

The proliferation of weapons has really affected the security and peace of the contemporary global system. An average of $2.8 trillion is spent annually on security and defence, the bulk of which goes into production and procurement of arm facilities. If such amount of money is spent on the alleviation of poverty annually, I am very convinced that in five years, there would be no case of poverty anywhere in the world, even in the most remote part of the world, not even shown on the world map. Despite the debt regime being faced by most states in Africa, Africa's budget on defence is still very high. This patronage has even attracted more investors into the area of arms production, posing a danger to national and world security.

The large quantities of small arms and light weapons looted from the Army armoury in 1997, has resulted in the breakdown of law and order in Albania. But the UN intervention saved the nation from total political collapse. In 1998, the UNDP developed a community based programme in Gramsch, Albania where illegal arms were surrendered. The organization embarked on local development projects like road repairs, and telecommunication build-ups, which were labour intensive, affording the civilians, a great opportunity to be gainfully employed. The UNDP incentives made the demobilization process a success.

After the end of the civil war in El-Salvador, an average increase rate of 36% was recorded on annual basis in the country on homicide related incidents. This has given the police in the country a great concern considering the high risk involved in the combat of this menace and management of security. It is no surprise that, most foreign investors usually think twice before investing in the country because of the endemic insecurity existent. Mozambique is another country where there are over 10 million AK-47 assault riffles in circulation. An AK-47 riffles in Mozambique costs less than $100. This has made management of security in Southern Africa a great task, as the incidence of violent crimes has astronomically been on the increase.

In West Africa, the civil wars in Sierra-Leone and Liberia have had some spilling effects on the neighbouring countries. Cote d'Ivoire, a once relatively peaceful country has joined the league of post cold-war civil strife countries in the sub region. The country is still trying to cope with insurgent attacks from the rebels, achieving a positive peace still remains off sight. The crime rate of banditry, arson, communal conflict, religious crisis and assassination has gone up in Nigeria since 1990s, when the war in Liberia became intense. Liberian civil war has contributed to proliferation of small arms and light weapons in the neighbouring countries including Nigeria (Bar, 2005).

However, the use of sophisticated and deadly weapons by criminals is experienced both locally and globally. For instance, insurgent bombing and shooting in the Niger Delta region of Nigeria and violent armed robbery attacks like *Idi-Ape* bank robbery incident in Ibadan where many innocent civilians and policemen were killed by the robbers, have shown the destructive nature of modern weapons used and their high capacity to undermine the security of any people or communities. On international front, the danger that proliferation of weapons pose to security of lives and property was displayed in several ugly events like the London bombing, the 'unbomber' incident in the US, Coke Prince operations in Columbia, bombings in Egypt, the Basque bombings in Spain; among others. Some of the terrorist organizations in the world have even adopted the use of chemical weapons like Anthrax against their target population. The United States of America experienced incident of anthrax attacks on some of its citizens, just after the Sept. 11, 2001 terrorist attack on the US.

The initial demobilization exercise supervised by ECOMOG that took place in Liberia failed because, there were still many arms in circulation among the civilians and another reason was that the Taylor ex-combatants were not demobilized, which created a room for suspicion, which later (among other reasons) resulted in another outbreak of armed conflict in that country. That development nevertheless thwarted the efforts to effectively reconstruct post conflict Liberia for lasting peace and security in Liberia until the end of Taylor's rulership.

Somalia is another case study where over-circulation of arms among the people has led to the collapse of political institutions in that country such that there is unstable government. The phenomenon of piracy resulting from the activities of several criminal gangs in that war-torn country has been a source of worry to the world at large. Many ships' owners and workers have fallen victim of the nefarious activities of the Somali pirates. Nigeria has its bitter tale from the criminal activities of these pirates as captioned by Afrik.Com as follows:

Nigerian sailors captured by Somalian pirates have been released after ten months in captivity. A group of government delegates have been dispatched to Yemen to facilitate the return of the freed sailors. The pirates demanded a one million dollar ransom, but it is not clear if any ransom has been paid (://en.afrik.com/article 15791.html)

There is no doubt that absence of government in true sense since 1991 resulting from the endless civil war that has been plaguing the country for almost for almost two decades has contributed to over-circulation of arms and weapons among the Somali population. There has been a great challenge on the government (with political power) to ensure security of lives and property. The country is experiencing humanitarian crisis and it remains one of the highest contributors of refugees on the continent of Africa. All efforts by African Union and other peace stakeholders have continued to be fruitless because of the presence of large number of arms and weapons among the people. It is only when effective disarmament and demobilization is attained that the security of lives and property can be guaranteed in that war-torn country.

By and large on the issue of distribution pattern, we can say that distribution pattern of arms proliferation can either be **vertical** or **horizontal**. Horizontal distribution pattern involves the distribution or access to arms by all state and non-state actors. Weapons that can be found at this level may include small arms and light weapons. On the other hand, vertical distribution pattern usually involves large weapons or weapons of mass destruction like nuclear weapons, which are limited in access and production. It is the world powers like the US, Russia, among others that can produce and access these weapons due to the very destructive impact that the use of such weapons can have on the world population and environment. Non-state actors and weak or less powerful states are also barred from producing or/and accessing it. But, the recent development is that some other states not officially in the league of nuclear powers have began to embark on building nuclear plants and there is high suspicion that these countries can either be careless or reckless in the handing of these deadly materials especially if terrorists find their way into possessing them.

SELF ASSESSMENT EXERCISE

How do you describe the present state of small arms proliferation in your country?

4.0 CONCLUSION

The devastating effects of arms proliferation are enormous and have necessitated the need to always call for global attention in the maintenance of security. Quite a number of research and policy plans have been developed to address the devastating effects of arms proliferation problem in the contemporary world system. Some instruments of disarmament have been developed and ratified by several nations of the world with the aim of promoting peace and security. There have persistent commitments by the UN Security Council, United Nations at large, regional and sub-regional organization, to always facilitate and maintain a series of Arms Limitation Treaties as a way of fostering world peace and security.

5.0 SUMMARY

In this unit, we began our study by explaining the meaning of arms production and proliferation. We also traced the origin of the current proliferation of arms/weapons undermining national and international security to the World wars and 1945 emergence of the Cold War. We went further to examine distribution pattern of the proliferated arms/weapons in the global system and the attendant negative effects it has on the capacity of governments to maintain security in their various countries.

6.0 TUTORED MARKED ASSIGNMENT

i) What is arms proliferation;
ii) Briefly discuss the history of arms proliferation; and
iii) Describe what you understand by arms distribution patterns.

7.0 REFERENCES/FURTHER READINGS

Bar, M. S, (2005). West Africa: From a Security Complex to a Security Community. *African Security Review* 14 (2). Also available on ://www.iss.co.za/index.php ?link_id=3&slink_id=1936&link_type=12&slink_type=12&tmpl_id=3. Retrieved on 3 December, 2009.

Boutros–Ghali, B. (1992). *An Agenda for Peace*. New York: United Nations.

DFID (2003). *Small Arms and Light Weapons*. A UK Policy Briefing.

Green, W. & Punnett, D. (1963). *MacDonald World Air Power Guide*, Garden City, New York: Doubleday & Co.

Lieuwen, E. (1961). *Arms and Politics in Latin America*, New York: Praeger

Roberts, C. M. (1974). The Road to Moscow. In: Willrich, M & Rhinelander, J. B. (eds.). *SALT*: *The Moscow Agreements and Beyond*. New York; The Free Press.

Sutton, J. L. & Kemp, G. (1966). *Arms to Developing Countries: 1945-1965*. London: Institute of Strategic Studies.

The Nairobi Declaration on the Problem of the Proliferation of Illicit Small Arms and Light Weapons in the Great Lakes Region and the Horn of Africa, March 2000.

Treverton, G. F. & Bennett, B. W. (1997). *Integrating Counter-Proliferation in Defense Planning*. St. Monica: RAND. Issue Paper.

United Nations (2000). *We the Peoples: The Role of the United Nations in the 21st Century*. Millennium Report.
Worldwatch Institute (1997). *Small Arms Proliferation: The Next Disarmament Challenge*. 25 October. Also available on ://www.worldwatch.org/node/1615. Retrieved on 7 September, 2009.

://en.afrik.com/article 15791.html. Retrieved on 2 September 2009.

.news.amnesty.org/index/ENGAMR360112005. Retrieved on 2 May 2007.

.en.wikipedia.org/wiki/Small_arms_proliferation. Retrieved on 2 May 2007.

.globalpolicy.org/security/smallarms/articles/2003/0630menace.htm. Retrieved on 2 May 2007.

.prospect-magazine.co.uk/list.php?subject=151. Retrieved on 2 May 2007.

.smallarmsnet.org/issues/themes/armsprol.htm. Retrieved on 2 May 2007.

.thenation.com/directory/nuclear_arms_proliferation. Retrieved on 2 May 2007.

.worldwatch.org/node/1615. Retrieved on 2 September 2009.

UNIT 5

WAR AS A SECURITY THREAT

CONTENTS

7.0 References / Further Reading

1.0 INTRODUCTION

Since the collapse of the Soviet Union, marking the end of the Cold War era, security discourse and practice has undergone a number of transformations. There has been a paradigm shift in the analysis of security issues in recent times. It is noticeable that new security threats have emerged, as non-state actors appear to pose greater security risk to national and international communities. The hopes of having a global system that will be devoid of war and violent crimes by many quarters, have been dashed considering the state of the world polity where perpetual insecurity has become the order of the day.

The very virulent nature of emerging security threats has been a source of worry to governments at all levels (from local to global). The growing loyalty of people towards sub-state entities and the pervasive attitude of ethnic nationalism and ethnocentrism have been undermining the potential of countries like Nigeria to effectively manage internal security, reducing the capacity of the government to achieve nation-building. The relevance of the security sector in the maintenance of law and order in Africa especially has been a subject of debate. The recent incident of *Boko Haram* crisis in northern Nigeria especially Borno and Bauch states where some anti-Western education Muslim fanatics engaged security agents in bloody battle, a situation that led to more than 1,000 deaths.

The unprofessional handling of the situation by the Nigeria Police raised a doubt about ability to manage crime and overall internal security of the country. If the excesses of the *Boko Haram* sect had not been checked by the law enforcement agents (especially the Army), the group may later have decided to engage Nigerian state in Jihad (holywar) as a way of challenging its secularity. In this unit, we shall be studying war as a threat to security. Owing to the danger that war poses not only to the people but also the environment, it is germane to put in place relevant security strategies and policy actions that can assist in mitigating the threat of war.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Define the term war;

Describe the features of war; and

Explain the categories of warfare.

3.0 MAIN BODY

3.1 **Definition of War**

The term war is often given some interpretative connotations ‘whose meanings, rarely examined’ (Smith, 1989:23). The conceptualisation of war has remained problematic in international relations. It has been greatly flexible and dynamic. War may be described as open armed conflict between nations or states or between parties in the same states, facilitated by force of arms for various purposes. Thus, there exist specific parameters to define the concept of war. According to Professor Tunde Adeniran, war involves:

……. common agreement, that is distinct from peace, and it is characterized by military activity, high social and political tension, and the breakdown of normal relations. War could result from a deliberate and carefully calculated decision… It could also be a choice among alternative courses of action and could be only course one is left it. It is a phenomenon which affects everybody and all nations, irrespective of ideologies, and irrespective of the level of economic and political development (Adeniran, 1982: 123).

War can also be defined as protracted state of violent, large-scale conflict involving two or more parties. War is aggression and counter-aggression whose chief property is large scale destruction both in human and material terms within the context of time and space. According to Carl Von Clausewitz, “It is of course well known that the only source of war is politics .....war is simply a continuation of political intercourse, with the addition of other means” (Clausewitz, 1982: 119).

War has remained a regular feature in human civilization. It often spices the relationship between parties, and in spite of its virulence and danger to continued existence of man, war has remained recalcitrant in human history. War spices every century, race, continent, nation, society and culture, which makes it pretty impossible to study human history without taking a look at the activities and actions of man, which have aroused a violent conflict behaviour as well as the role played by upsurge of the war situation in shaping the relationship among various state and non-state actors. Thus, considering the foregoing, one tends to agree with Clemenceau as quoted by Andreas Osiander (1994):

From the most remote ages onward, the peoples have perpetually assailed one another for the satisfaction of their appetites and their egoistical interests [and their fears (Osiander, 1994:265)

Nonetheless, wars vary in intensity. We have **high intensity warfare** and **low intensity warfare**. High intensity warfare is between two superpowers or powerful countries fighting for political goals. Low intensity warfare involves counterinsurgency, guerrilla warfare and specialized types of troops fighting revolutionaries.

SELF ASSESSMENT EXERCISE

How do you describe the term war?

3.2 Features of War as a Security Threat

The experiences of the 20th century have shown that the century recorded more war with incomparable human casualty than previous centuries put together. According to Gray (1999), the century produced two world wars, a handful of international wars, cold war, anti-colonial insurgence, ethnic violence among others. The century also marked the beginning of sophisticated and lethal technology in weaponry and prosecution of war. The emergent war technology has presented the world as unsafe not only to man but also the general ecosystem. The underlying threat that war poses to security of lives and property of any people is very high, as captioned by Braden and Shelley:

War has been as analogous to disease in its spread and effect. It has been likened to natural disasters in its impact on society's structures (Braden & Shelley, 2000:69)

Similarly, the view of Braden & Shelley (2000) was further illuminated by Osisioma Nwolise who argued that:

War destroys life, and property, principles and values, and wakes up beastly elements in man. War leads to environmental pollution and degradation. It kills human beings in their millions depending on the magnitude.....and forces people to leave their homes and become refugees in their country or outside. War diverts the developmental resources of a state to defence and war-making. It retards the rate of development of a people and a state, at least in the short-run. It spreads pestilence, destitution, hunger and starvation. It creates gross insecurity and traumatises people (Nwolise, 2004: 8).

Clausewitz in his axiom argues that the relationship between means and objectives of war involves a situation where the latter remains paramount throughout the war. Clausewitz also describes the war environment in his 'climate of war' as having four features, which include **danger**, **exertion**, **uncertainty** and **chance**, concluding that war is both deadly and a gamble. To stimulate our better understanding of the subject matter, it is quite imperative to examine the above mentioned features of war as presented by Clausewitz.

Danger of War

On danger of war, no one will disprove the damaging and destructive implication of war not only on human beings and material resources but also on the entire ecosystem. The tendency for mutual destruction is high. The danger of war is not limited to the combatants but also extends its virulence and social venom to parties not directly involved in the conflict or not involved at all.

A good example was the Sierra Leone Civil War, which began in 1991 where several thousands of innocent civilians lost their lives as more than 2 million people (well over one-third of the population) were displaced. Neighbouring countries became hosts to a significant number of these displaced persons as refugees while trying to escape the civil war.

The civil war was initiated by the Revolutionary United Front (RUF) led by Foday Sankoh. The rebel group (RUF) launched its first bloody campaign into eastern Kailahun of Sierra Leone from Liberia on March 23, 1991. In less than five months, the crisis had generated about 107,000 refugees who fled the conflict into Guinea (Adebajo, 2002:90). Foday Sankoh was the head of the military wing of the RUF that included in its ranks Burkinabes and members of the National Patriotic Front of Liberia (NPFL) under the tutelage of Mr. Charles Taylor.

The civil war in Sierra Leone featured conscription of Children by the RUF rebel group in the recruitment of its army, sexual slavery, murder of non-combatants among other war crimes. Nevertheless, such acts were tantamount to the contravening various international conventions and protocols guiding the conduct of war.

However, it is not surprising that the chief co-conspirator in such shameful and dastardly act, Charles Taylor is now facing trial at the Hague over alleged war crime offence, and if he is found guilty he may spend the rest of his life in prison. It is important to note that not all the leaders of the RUF particularly the intellectuals among them supported the rebel strategy adopted by Sankoh. Many of them berated and condemned forced recruitment of children although a lot of these disentting voices were brutally murdered by Foday Sankoh. The war led to the collapse of all state structures with attendant socio-political disorder and structural cataclysm.

A numbers of scholars have blamed the upsurge of the crisis basically on the irrational desire of the political gladiators to exclusively enjoy the control of Sierra Leone's diamond industry (Hirsch, 2000: 15). The endemic poverty, which reigned supreme among the mass public also contributed. Thus, the majority of people were subjected to marginal survival as chronic penury remained second nature.

The 1999 Lomé Agreement failed to restore any peace in the country due to the strategic advantage it gave the RUF rebels as Foday Sankoh was put in charge of the mineral resources of the country, meaning that the diamond trade was largely under the control of the rebels. The attempt made by the United Nations (UN) to reduce the rebels’ control of the diamond fields was greeted with resurgence of the civil war. The situation of insecurity became deepened. The RUF resorted to carrying out an offensive campaign against the UN troops. It took the intervention of the British troops to save the country from persistent bestiality in the hands of the rebels. The British military intervention in that war-torn country is commendable owing to the success it recorded in the restoration of peace and security in Sierra Leone.

The rebel leader was captured and the British left a training team to rebuild the armed forces of Sierra Leone as effective institution for sustainable post conflict state security. British actions were instrumental to eventual American intervention in Liberian war. It is a fact that the termination of armed hostility in Liberia has really helped in providing stability on Sierra Leone's borders and restoring normal market forces to the diamond trade.

The danger of war in West Africa could be observed in the volume of refugee generation in the region, which has increased trans-border crime, armed robbery and wide circulation of small arms and light weapons among the civilian population making the prevailing atmosphere of peace a fragile one. The number of small arms in Nigeria has increased tremendously since the outbreak of war in Liberia in the early 1990s.

The inherent danger in the outbreak of war in any country is instructive to the activities of the neighbouring countries in making sure that peace is restored in the warring state because of the potentials of such war, in spreading to the neighbouring countries. Great Lake region is a good example where war has become an infectious disease plaguing the countries in the region, which makes the region the highest generator of refugee flow on the African continent. The region has had the lion share in the flows of refugees in Africa. The countries that we find in this region include Burundi, the Democratic Republic of Congo (DR Congo), Kenya, Tanzania, Rwanda and Uganda. All these countries at one time or the other have contributed to the production of refugees in the region except Tanzania (see Afolayan, 2003; Evans, 1998; UNHCR, 1991).

Exertion

Exertion is the act of putting some power or faculty into vigorous action. War saps energy as it involves both mental and physical strength. Soldiers are disciplined and drilled for the task they will face in the theatre of war. It is no question that anybody recruited into the military must be physically fit and be emotionally stable. War is not a joke, it is serious business!

There are some light weapons that an average man cannot carry. Not every adult can withstand operating an AK-47 riffle because of the pressure it exerts. Apart from the physical strength that is required in any anticipated successful military campaign, the troops or belligerents must also have an advantage in the area of tactical support capabilities, which puts the mental ability at work.

Also, war consumes a lot of socio-economic resources. In Iraq war, the US and its allies must have spent nothing less than $30 trillion apart from human casualty being recorded almost weekly, if not daily, on the side of their (the US and its allies) troops. The war has really sapped the economy of the US to the extent that the country is said to be on the verge of economic recess.

Uncertainty

The power relation between the armed gladiators is viewed to often determine the outcome of a violent hostility. In a case whereby there is assymetric relation in the power equilibrium of the disputing parties, on average person will believe that the outcome of such conflict will always be in favour of the stronger party. It is often believed that in a situation of armed conflict between a great and weak nation, considering the military capability, mobility, and strategic superiority enjoyed by the former over the latter, the former (great power) would be the victor.

Carl Von Clausewitz disagreed with the above notion, arguing that war is not only risky business but is also coloured by uncertainty. The fiasco suffered by the US in the Vietnam war as well as the failure of the US and its allies to conclude the war in Iraq have given credence to the argument articulated by Clausewitz.

Despite the asymmetric power relation between Iraq and the US led allied forces, the war in Iraq has remained more prolonged than expected. This explains why a number of scholars in the fields of politics and conflict studies fondly say that the US and its allies have only succeeded in winning the war but not the battle. This is because the war has moved from conventional to unconventional violence. The number of the US troops being injured or killed on weekly bases by the local militants through guerrilla war strategy is considerably high.

Another example of uncertainty in the outcome of war is the Sino-Japanese War. The Sino-Japanese war was the first major international war involving China after 1860. The war was between China and Japan. The relationship between the duo had never been cordial even before the outbreak of the war. The cause of their armed hostility was the control of Korea. Korea had been a tributary of China for a long time. China was displeased with the bilateral diplomacy entered into between the Seoul government and Japan, an age-long rival.

The bilateral diplomacy became further cemented in the following years. Then emerged a clash of influence between China and Japan, when the former wanted to continue maintaining its traditional influence in Korea, the government of the latter was all out to consolidate the diplomatic relation between her and the Seoul government.

The gladiatorial posture was maintained by the duo of China and Japan until the emergence of full blown war between them in 1894. The war lasted for one year. Due to the size of the Chinese army and its naval superiority in the region, one would have thought that China would win the war convincingly but to the surprise of the entire world, Japan won the war. By 1895 a treaty was entered into the Treaty of Shimonoseki which held that:

China had to recognize the independence of Korea and had to cede to Japan the Island of Formosa, Pescadores Islands, and the Liaotung Peninsula (Strayer *et al.*, 1961: 318).

The world experience has shown that uncertainty is not limited to the outcome of war but it also curries every aspect of war policy. A good example is the Fashoda Crisis.

England and Egypt were in control of Sudan, and due to the local revolt led by "Madhi" Muhammed Ahmed, Britain decided to withdraw its administration of the State (Sudan). The Madhi's followers then took over the political administration of Sudan. Britain quickly rescinded its decision to leave Sudan, when she noticed that the French and Belgian colonizers were extending their imperial expedition towards Sudan, knowing fully well that its interest was likely to be jeopardised for no more reason than the headwaters of the Nile being controlled by the Sudan. By 1896, the British and Egyptian forces under the tutelage of Lord Kitchener began to reintroduce imperial administration in the Sudan. In 1898 Kitchener's imperial exploration approached the fort of Fashoda on the Nile, and discovered that French forces had already annexed the Sudan to France. Then, there emerged a tension between the British and French forces for the control of the Sudan.

The French rethought the war option because it considered its non-readiness to engage the British forces in naval war. Therefore, the French had no other option than to leave the Sudan. By 1899, the Britain and Egypt had established joint control of what later became the Anglo-Egyptian Sudan. The French conceded to England, not because of the fear to enter into war with England *per se* but the uncertainty that underlies war articulation.

Chance

Chance can be referred to as unknown or undefined cause of events not subject to calculation. According to Clausewitz (1982), war is a game of probability, or simply put, a game of luck. **War Weariness Hypothesis** makes us to understand that a country at war will definitely get tired and such country may lose the enthusiasm or zeal which is likely to restore an atmosphere of peace. If we take a critical look at this argument, we may support Clausewitz from the perspective that **party A** may decide to engage **Party B** in war while **Party B** had just experienced a protracted war situation with another party, and entering any prolonged war with **Party A** may be considered by it (Party B) as uncalled for, if it can make concessions that may not largely affect her interest for restoration of peace.

An example of this, is the anti-colonial armed struggle between the imperial forces of portugal and the Mozambican liberation movement-Frente de Libertacao de Mocambique (FRELIMO). FRELIMO was formed in 1962 and began its guerrilla operations in 1964. Their mission was basically to wrestle political power from the portuguese colonialists for the independence of Mozambique. At the time the anti-colonial struggle was going on in Mozambique against the Portuguese colonial force, Guinea Bissau's Partido Africano de Independencia Guiné e Cabo Verde (PAIGI), Guinea Bissau's armed liberation movement was also waging war against Portuguese colonialists in its home country. The two anti-colonial insurgent movements, FRELIMO and PAIGI took the risk of waging war against the Portuguese forces knowing that war weariness may set in, coupled with the political challenge Portugal was facing at home. It was believed that those two reasons might have forced the

Portuguese to accept their fate in the battle for supremacy. Eventually, Portugal had to abandon the countries.

Sometimes, the above-mentioned calculation may not work, considering that the activities of Germany after the First World War Germany was sanctioned and faced a great penalty for war-mongering. Although, the country still undertook a very risky adventure by going into another war in the realisation of the Nazist lebensraum project as well as other variables, nonetheless, it took the whole of Europe by surprise that despite the defeat Germany suffered in the World War I and its consequences on her, the country still embarked on offensive mission, which snowballed into World War II. Adolf Hitler took the risk to launch the German race into racial eminence and superiority but he, his Nazist Gestapo and the entire Germany became the victims of their own (war) policy.

SELF ASSESSMENT EXERCISE

Explain the features of war as posited by Clausewitz.

3.3 **Categories of Warfare**.

There are two major categories of warfare. These include conventional warfare and unconventional warfare. For **conventional warfare**, it involves well-identified, armed confrontation between parties. A good example is the Iraq war, i.e. the early part of the war when the allied forces led by the US and Britain engaged the Iraqi regular soldiers and irregular forces in an open military campaign. This kind of open armed confrontation is supposed to be devoid of application of weapons of mass destruction as mandated by the laws of war and several other conventions.

Unconventional warfare refers to any armed conflict that does not involve the parties engaging in an open confrontation. This category of warfare is often adopted mostly in a situation whereby the combatants have asymmetric power relation. After the defeat of the Iraqi forces in an open armed hostility, many of the Iraq soldiers that survived the military onslaught by the allied forces went underground.

Many of the old Iraqi guards are responsible for the guerrilla offensive being carried out against the allied forces as well as the local people. The reign of terror pervades the entire post-Saddam political landscape in Iraq. This category of warfare usually involves tactics like raiding, terrorism, insurgency, guerrilla, even as well as nuclear, chemical or biological warfare.

SELF ASSESSMENT EXERCISE

What are the categories of war?

4.0 CONCLUSION

War remains a great threat to the security of any country. May be because of its devastating effect, it has continued to attract growing attention among scholars, policy-makers and militarists. It has become worrisome that since the beginning of the Cold War era, nationalist struggle and rebellion have been phenomenal in developing countries, especially of Africa leading to a series of civil wars and insurgencies as experienced in Nigeria, Sierra-Leone, Angola, to mention a few. The incident of genocide mounted by the inter-ethnic violence in Rwanda continues to be a nightmare. The capacity of the security sector to maintain law and order has persistently been undermined by local insurgents and rebel forces. This situation has posed a great challenge to security management in Africa.

5.0 SUMMARY

In this unit, we discussed the meaning of war and showed how it constitutes a threat to security of any people or state in our conceptual definition. Thereafter, we explained various features of war with credence to the intellectual contributions to the study of war by Clausewitz (1982). The third and last area of discourse about the subject was to explain the basic categories of warfare: conventional and unconventional. Thank you for your patience and the zeal you have demonstrated since the beginning of this unit to acquire knowledge.

6.0 TUTORED MARKED ASSIGNMENT

Define the term war and explain the features of wars as articulated by Clausewitz.

7.0 REFERENCES / FURTHER READING

Adebajo, A. (2002). *Liberia's Civil War: Nigeria, ECOMOG, and Regional Security in West Africa*. Boulder: Lynne Rienner Publishers.

Adeniran, T. (1982). *Introduction to International Relations*, Lagos: Macmillan Nigeria Publishers Limited.

Afolayan, A. A. (2003). Dynamics of Refugee Flows and Forced Repatriation in Africa. *African Journal of Peace and Conflict Studies*. 1(1): 66-90.

Braden, K. E. & Shelley, F.M. (2000). *Engaging Geo-Politics*. Harlow:Prentice Hallsee.

Clausewitz, C. V. (1982). *On War*. London: Penguin Books.

Evans, G. (1998). Responding to Crisis in the African Great Lakes. *Forced Migration Review*, 1: 32-33.

Gray, C (1999), *Modern Strategy*. Oxford: Oxford University Press.

Hirsch, J. L. (2000). *Sierra Leone: Diamonds and the Struggle for Democracy*. Boulder, CO: Lynne Rienner Publishers. (December 1).

Nwolise, O.B.C. (2004). *The Nigerian Police in International Peace-Keeping in a Changing World*. Ibadan: Spectrum Books Limited.

Osiander, A. (1994). (quoting Georges Clemenceau December 29, 1918), *The States System of Europe, 1640–1990*. Oxford, UK: Clarendon Press.

Smith, R.S. (1989). *Warfare and Diplomacy in Pre-Colonial West Africa* (2nd Edition). London: James Currey Ltd.

Strayer, J.R., Gatzke, H.W. & Harbison, E.H. (1961). *The Course of Civilization* (Volume Two). NewYork: Harcourt, Brace and World Inc.

UNHCR (1991), *Refugee Survey Quarterly*, Geneva.

MODULE 3

UNIT 1

SAFETY MEASURES TO THE MANAGEMENT OF NATURAL THREATS

CONTENTS

1.0. INTRODUCTION

In the last five units our attention has been drawn to some major security threats. Our studies covered crucial aspects of these security threats. Apart from those threats considered to be manmade and natural, we also discussed some other kinds of threats, like information warfare. In this unit however we shall attempt to provide some safety tips in the management of natural security threats or hazards. The rationale behind our decision to explain some of the ways to manage these natural threats or hazards is to advance the knowledge on safety ideas and practices that can help us to mitigate the effect of any major natural threat. Let us quickly go through various tasks that we need to undertake in this unit in the objectives of the study.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Explain safety measures in the management of earthquake;

Discuss safety tips useful in managing flood;
Describe the essential safety steps to managing hurricane; and

Elucidate on safety instructions in preparing against and responding to drought.

3.0 MAIN BODY

3.1 **Safety Measures against Earthquake**

Earthquake is an unexpected and hazardous vibration resulting from the sudden shake of the Earth's crust. It is usually caused by rupture of geological faults but nuclear experiments, landslides, mine blasts as well as volcanic activity can also provoke the earth to quake. One important feature of earthquake is that there is no technology or electronic device that can adequately predict any occurrence of earthquake but some parts of the world are more prone to this hazardous situation than others. It is therefore imperative to present some of the safety tips that we can observe for hazard mitigation as follows:

Before the occurrence of earthquake

a) One of the safety tips to the management of earthquake before it occurs, is to always ensure that you equip your homes with drinking water, adequate food (particularly the non-perishable food items like rice), transistor or any mobile radio with ordinary or rechargeable batteries, torch with batteries, as well as first-aid kits.

b) It is imperative to educate the public on how to manage their home appliances and build in themselves the culture of safety like switching off electricity or/and gas cooker or/and electrical appliances when these are not in use. Apart from safety, such culture helps families to save money, which would have gone into settling of huge energy bills as well as conservation of energy.

c) It is also important to prepare yourself towards mitigating the effect that earthquake may have on your household by identifying places in your house that can be used as cover in the event of occurence of earthquake (://kashmirdivision.nic.in/Disaster_ Management/dm_center.htm).

d) You are also expected to always have your phone charged and you should endeavour to keep the backup copy of the list of contacts on your phone in a separate place most preferably a book. So, when your phone is misplaced or stolen or destroyed, you can still have a backup through which you can access your list of contacts. By having the contacts, you can easily contact any other relative(s) or friends to alert him/her of the situation of earthquake. By doing this, you will enable others to reach you to monitor the state of safety of the affected person(s). Apart from that, you will be able to alert others who may be coming to the place of the prevailing hazardous circumstance with the aim of reducing casualty. Here, one will be expected to call relative(s) or friend(s) that are far away from the site where the hazard is taking place.

e) If you are relocating to a location prone to earthquake, you should ensure that the house is retrofitted with earthquake safety measures. One of the ways to do this, is by “reinforcing the foundation and frame” (**Error! Hyperlink reference not valid.**). These measures can help to make the house resistant to quivering. It is therefore advisable to always contract qualified building and structural engineers before you do your construction.

During the incident of earthquake

As we may already have been aware, earthquake is one natural hazard that cannot be predicted by any modern technology. Often times, when an earthquake is about to occur, there is a loud sound indicating its arrival. One is only left with very little or no time to prepare against the hazard and any important steps that you take at this material time will go a long way to determine how much you will be able to mitigate or reduce the losses that such a hazard may attract. During the hazard, it is expected of you to know some important steps to take so that the hazardous situation will not have too negative or destructive an impact on you and those around you. Steps to take should include:

a) You should take cover by looking for a very safe place where you can veil yourself against any falling objects like walls, ceiling fans, etc. It is advisable to lie under a table or well-built furniture, and be smart enough to move when it moves. You should also make sure that furniture are well positioned to prevent them from stumbling;

b) You should also avoid standing in doorways because of the possibility of having violent motion slamming the door against you. Avoiding this will also guard you against being hit by any flying objects, some of which may be very deadly;

c) Endeavour as much as you can to move away from windows, mirrors, book shelves, or any place where heavy objects can fall on you. As we have said earlier, the major destruction does not emanate from earthquake itself but by the conditions that occasion it. One of the conditions is vibration that can fall heavy objects as well as walls of the buildings and the buildings themselves. For instance, if someone has some giant lightening equipment hung on the ceiling, and earthquake occurs, there is the possibility that such heavy lightening decorator will fall off the ceiling, which can lead to the injuries or even death if it fall on a person. This shows that we need to consider the geophysical conditions of a place before we decide on the decorations that we can use to beautify our houses;

d) If you find yourself in a tall building, avoid using the lift to get out of that building. It is advisable rather that you negotiate your escape from such building going through the stairs. The emergency nature of this hazard (earthquake) does not usually give much time for evacuation. Therefore, you can stay where you are or better-still proceed to the uppermost floor of the building if the task will not be strenuous. This will afford you an opportunity to be reached by an emergency if there is a case of collapse of the building. The rescue teams usually reach the victims on the uppermost segment of the rubble;

e) If you are outside, ensure that you are in a open place where no buildings or electric wires and poles or trees or street lights or telephone facilities or any other heavy objects can fall on you or get you electrocuted;

f) In a situation whereby a home damage is experienced, you are advised to leave the premises and make sure that you have drinking water, food, medicines as well as essential documents with you as you leave. The reason is not far-fetched, there is likelihood that the vibration might have weakened the foundation of the house, and the collapse of the house is not unlikely. It is therefore important to vacate such a house until after the hazard when the services of building experts will be required. The building experts and engineers will investigate if the foundation of the building has been (badly) affected by the quake. If it is affected, it is advisable to pull down the structure to avoid further casualty. This is one of the challenges being faced in post-hazard environments. It is incumbent on the government to assist the victims with alternative housing, and there should be emergency funds to assist the victims in the reconstruction of their homes;

g) It is also important to distance oneself from any electric wires and avoid touching any metals especially those in contact with electric cables. The reason is that there may be electric current in those wires and metals, capable of getting anybody that touches any of such objects electrocuted;

h) Another safety measure bothers on being on transit probably in a vehicle. Here, you are expected to disembark from the vehicle or soon as you find somewhere safe to park. The place should be far away from buildings, trees, streetlights, electric poles, or other objects that may considered to have potentials to harm you; and

i) Similarly, you should avoid using bridges whenever you are aware that a situation of earthquake has occurred in a place. This is because there is likelihood that the base of the bridges may have been affected or badly damaged by the quake.

After the incident of earthquake

a) Due to the presence of debris in the aftermath of earthquake, you are advised to wear cover shoes to avoid your feet being exposed to any dangerous particles or sharp objects that may get you injured or infected;

b) It is important to also note that after initial tremor from the earthquake, in the coming days, week or even months, aftershocks can make weakened structures to collapse. So, if one hears a tremor emanating from the sound of collapsing structures, one should not get traumatised, and should expect such to happen in the aftermath of an earthquake;

c) As a result of the foregoing, it is pertinent to vacate all the buildings affected by the quake until their conditions are ascertained by the relevant building engineers. If one’s house is found to be structurally damaged, it is expected that the person and his/her co-occupants should immediately vacate the building to prevent avoidable deaths or injuries;

d) The use of battery-operated radio and torch can come in handy because the effect of the tremor may also include damage of electric facilities, leaving the affected areas in blackout. However, you can use your touch to see and the radio will serve a significant purpose of allowing you to monitor events right from where you are. The interviews and comments by emergency experts invited on a radio will definitely go a long way to influence your actions towards making effective decisions in mitigating the effect of the hazard on you and other people who are with you;

e) If you are still stable health-wise, it is incumbent on you to render some voluntary humanitarian assistance and support to other victims that are trapped or injured and urgently need help and medical care. You are expected to take some roles to complement the activities of the emergency workers, and always adhere to experts' instructions in the evacuation exercise, so that you will not complicate the health conditions of any injured victim;

f) If you notice any electric spark, urgently reach out to the authorities concerned to intimate them of the incident. The rationale behind this is to notify the power authorities of the danger that continued supply of power to the affected area can pose to the victims of the earthquake. It is very essential on the part of the power authorities to cut-off supply of electricity to the affected area to avoid electrocution of any victim(s) of earthquake; and

g) Post hazard reconstruction should be carried-out by government and other humanitarian organisations like Red Cross, and all necessary cooperation be extended to them by the affected community.

SELF ASSESSMENT EXERCISE

What are safety measures to earthquake?

3.2 Safety Measures against Flood

Flood is another type of natural threat. It usually involves submerging of land by overflowing water. The following are of the safety measures to manage it:

Before flooding

a) If you know that you are staying in a flood-prone location especially those locations that are very close to the sea or river or big dam, it is germane to discuss with members of your household on how best they can act in the event of flood, so that they can be prepared ahead of such occurrence. This will definitely afford them the opportunity to act appropriately, timely and effectively in reducing the losses that a flood hazard may bear;

b) Sometimes, the incident of flood appears without notice, it is therefore important to identify the safest route to escape the ravaging flood;

c) It is always advisable to have protective equipment at home. For instance someone who knows that he/she lives very close to a river and considers the likelihood of flooding that may be occasioned by overflow from the river especially in a situation of continued heavy rainfall, should know that it is important to have protective equipment (like life jacket, first-aid kits, etc) at home;

d) Again, if you are staying in an area prone to flood, you should ensure that the drainage is well constructed and the materials used in the construction should be of very good standard such that they can withstand the threat emanating from the hazardous incident (flood). The use of mud walls should be discouraged due to their vulnerability to floods;

e) The culture of dumping wastes into canals should be absolutely discouraged, and erring members of the community must be reported to the law enforcement agents; and

f) Always promote the habits of switching off your electrical appliances when not in use. Whenever you are leaving home/office, make sure that you switch-off all gadgets and electrical appliances, or even turn off the power source (switch box).

During floods

a) Due to the overflow of water, there is tendency that some sewer systems will be badly damaged, which is capable of causing widespread diseases like cholera. It is therefore important to always cover your food and avoid taking untreated water;

b) If a case of diarrhoea is reported, you can use rice-water or raw tea or even tender coconut water to arrest the situation and immediately consult the health workers or emergency health practitioners you can find around for further assistance (://kashmirdivision.nic.in/Disaster_Management/dm_center.ht m);

c) You should always apply disinfectant solutions like Izal to clean your surroundings. The use of lime and bleaching powder can also be useful in the cleaning;

d) Ensure that you and other people in your household wear covered shoes to avoid infections;

e) Remove all valuable items including your electronic gadgets from the floor to a safe platform like bed to avoid getting them damaged by the water;

f) You are expected to provide necessary assistance to relief workers especially in the distribution of relief materials to other flood victims;

g) If you consider that it is risky to continue staying at the flood location, you can quickly and carefully embark on evacuation. If you have a car and you are sure that it can safely go through the water, you and your family can therefore leave but make sure you pack some of your important belongings like school results/certificates, warm clothing, emergency kit and other valuables in waterproof bags;

h) Ensure that you switch-on your radio to monitor the flood situation as you leave the flood location and turn-off the power in your house before you leave; and

i) Avoid getting into water that you cannot ascertain the level of its depth and current to prevent drowning or being taking away by water.

After flood

a) Avoid going about in flood water and be careful when it is mandatory for you to go out. Make sure that you have a long stick with you to protect yourself against snake bites. The reason is that if a place with large population of snakes is flooded, the incidence of snake bites becomes very imminent;
b) Discourage children from playing in the flood water because of the possibility of getting infection or even catch cold in the process or in the aftermath;

c) Avoid using any electrical appliances enmeshed in water until technicians have instructed that they can be powered and used;

d) Always stay glued to your radio to get updates on the incident of flood;

e) Monitor the children when they are eating so that they will not eat any food that has fallen into the water to avoid cholera;

f) The use of protective shoes is also very essential to avoid infections like rashes; and

g) You should always boil your water and avoid taking any untreated water.

SELF ASSESSMENT EXERCISE

Discuss the safety tips to flood.

3.3 Safety Measures against Hurricane

Hurricanes produce destructive surface winds and storm surges. High winds often bring about huge structural and environmental damage, as the storms are usually the most destructive component of a hurricane. The safety measures to the management of hurricane or mitigating its effect may include the following:

Before the Hurricane

a) It is expected for you as a security practitioner to be inquisitive especially striving to know everything around you. If you find yourself in a place, you should seek awareness on the hurricane risks peculiar to that area. You should also seek information on the storm surge history and elevation of the area;

b) You should seek information about the location of official shelters in time of hazardous incident before-hand;

c) You should ensure that there are necessary emergency kits and protective equipments available in your home and office, so that in time of hazard or hurricane threat, you will be able to respond more effectively;

d) If your area is vulnerable to hurricane attack, ensure that your home has a very solid foundation to withstand any pressure coming from the hurricane;

e) You must always trim down the various trees you have in your premises to avoid a situation whereby trees will damage the building as result of the effect of hurricane;

f) You should also equip yourself with transistor or battery radio, so that when there is incident of hurricane or any other threat, you will be able to monitor the event and get advice from experts featuring on the radio, speaking on the hazardous situation. Following experts' advice may be useful in mitigating the effect of the hazard;

g) Unlike earthquake, hurricane can be predicted and it is imperative on the part of government and other stakeholders to initiate moves to purchase necessary gadgets and equipment, which can monitor and predict the occurrence of hurricane. In most developed countries such facilities are existent, but contrary is the case in most African countries. Meanwhile, through globalisation of media and communication, through the internet, one can get the forecast if there is likelihood that hurricane will occur in a place;

h) If the news of any potential hurricane incident is made public, it is important to act promptly but also call two or more people to ascertain the authenticity of the information. Yet, if you are not sure, you can still reach the emergency agency in your country or neighbourhood or tune your radio to the stations where you can verify the information;

i) When you have confirmed that hurricane is about to occur, make sure that you seek information on the intensity of the hurricane before you make a final decision on the action(s) to take in responding to the hazardous event. If the hurricane is going to be very intense, it will be advisable to relocate temporarily from the hurricane site without wasting time;

j) If it is predicted that the hurricane will be less intense or constitutes very little threat to the lives of dwellers in the affected place, you can stay but be in-door to avoid being hit by a flying object that can harm you;

k) If you are staying at home, ensure that you have sufficient food and drinking water that can last beyond the time predicted of the hurricane. It is also important to keep listening to radio to monitor the hazardous event; and

l) Always switch off all electrical appliances not in use, or better still switch off the electric circuit completely when the hurricane finally approaches;

During hurricane

a) You are advised not to stay at the affected place, if you are instructed as such by the authorities;

b) Due to possibility of strong winds can prove deadly by blowing and knocking one against dangerous flying objects, it is always advisable to stay in-door and close all windows and doors to the house;

c) Before the final arrival of the hurricane, if you are not sure of the strength of the building you are staying, it is more appropriate to look for another house where you can stay temporarily till the hurricane subsides;

d) If you are leaving your house, make sure that you have sufficient food, drugs and drinking water with you so that you will not become a burden to your host;

e) It is appropriate to turn off all electrical appliances not in use and make sure that you have battery-operated torch or/and lamp by your side, so that you can have something to lighten your apartment in the event of power-cut resulting from either damage occasioned by the hurricane or deliberate decision by the power authorities to avoid any situation of electrocution among the victims of hurricane;

f) You should move away from the windows and doors to avoid them slamming against you, thereby preventing avoidable injury or death;

g) For safety, you can also lie on the floor or under a sturdy object like table or bed if possible till the hurricane lasts. But, in a situation whereby the hazardous incident takes very long time, you can move to interior rooms (**Error! Hyperlink reference not valid.**); and

h) Due to possible damage of the sewer facilities, you are advised to avoid drinking water directly from the tap to avoid cholera and waterborne diseases. It is however very important to keep some water before the emergence of the hurricane, so that when damage of sewer facilities is noticed, you can drink only from the water you have already kept. And when you notice sewer damage, make sure to inform the relevant authorities, so that they can transmit the information to the rest of the public. This is one of the ways one can prevent an outbreak of waterborne diseases like cholera.

After the Hurricane

a) You should endeavour to stay put where you have sought for temporary shelter, or if you have stayed at your own house during the hurricane, you should remain there until you are informed by relevant authorities that it is safe to come out;

b) Always make sure that your radio or/and television is on, to monitor the situation and get necessary advice on which steps to take to help yourself and others in recovery from the hazardous incident;

c) Endeavour to keep other relatives and friends informed about the conditions under which you are, so that they will be aware of your safety;

d) Avoid taking water directly from the tap without being informed by the relevant authorities that it is safe to take the water. You should also treat or boil your water to avoid waterborne diseases;

e) If you wish to drive after the hurricane, make sure that you put on your radio in order to be updated of situation reports about the incident by relevant authorities. Avoid as much possible, the use bridges except when you are sure that they are not structurally weakened by the hurricane or flooding produced by the hurricane;

f) You should avoid touching or stepping on fallen electric cables/wires, or any metals in contact with electric cables to prevent electrocution; and

g) Do not use kerosene lanterns and candle until an expert certifies that there are no leakages in your gas, in order to prevent fire-outbreak.

SELF ASSESSMENT EXERCISE

What are safety tips to hurricane mitigation?

3.4 Safety Measures against Drought

The incidence of drought does not only affect individuals, it is a problem that affects the whole community because of the possibility of the affected community to develop some features that portray "Tragedy of the Commons" (see Walker *et al.*, 1991). This situation exacerbates the self interest of some individual who use the communal property maximally for their own benefits alone. Hence the adverse effect produced by such activities end up affecting not a few but the entire community. For instance, there are those individuals or corporate bodies that engage in activities that promote trapping of the atmosphere with greenhouse gases like carbon dioxide (CO_2) and water vapour (H_2O), which usually emits heat in the atmosphere, thereby causing climate change.

Recent and continuous change in climate has also provoked heat and severe drought conditions as experienced in most parts of Africa. The truth of the matter is that corporate bodies like oil companies emit the greenhouse gases that provoke climate change in their activities and exploration of crude oil. On the other hand, some individuals also involve in the cutting of trees (deforestation) as a business by selling the trees as woods for furniture or even firewood for cooking, creating a situation of environmental degradation thereby exposing top soil moisture to evaporation.

The bottom line is that it is usually few individuals that engage in activities that mount severe drought conditions but it is the whole community that suffers the consequences of drought especially shortage in water supply. Notwithstanding, drought is a normal phenomenon but it becomes a source of worry when it appears severe. It is against this background that it is imperative on all stakeholders to engage in actions and policies that mitigate drought and these may include the following:

a) As a result of the difficulty in knowing when droughts begin and how long it will last, a number of drought indicators will be required before we can finally make a decision on the ways through we can effectively implement our water-management plan;

b) After knowing the relevant indicators, water users can then develop necessary contingency plans through which decisions can be made on future economic investments (Hrezo *et al.* 1986: 47). Some of these indicators may include the Palmer Index (a drought severity index), historical data on the present water consumption and expected amount of water that may be needed in the nearest future especially where there is significant population growth like sub-Saharan Africa. We can also use as indicators stream flow as well as the level of subsidence or salt-water intrusion;

c) Local emergency unit and the water ministry should work collaboratively in developing viable policy framework and planning on effective management of water. It is germane on the part of the government to educate the masses on the need to conserve water and avoid waste of water resources;

d) It is also incumbent on government to alert the public if the incident of drought becomes noticeable. This will afford both individuals and corporate bodies to develop their own contingency plans towards addressing the water shortage that may be produced by the drought. With the aim of maintain sufficient agricultural production, construction of irrigation (known as *fadama* in northern Nigeria) can be useful. But, the prevailing pollution of water by several individuals and industries in Nigeria has also undermined the relevance of irrigation as an alternative source of water for plantation;

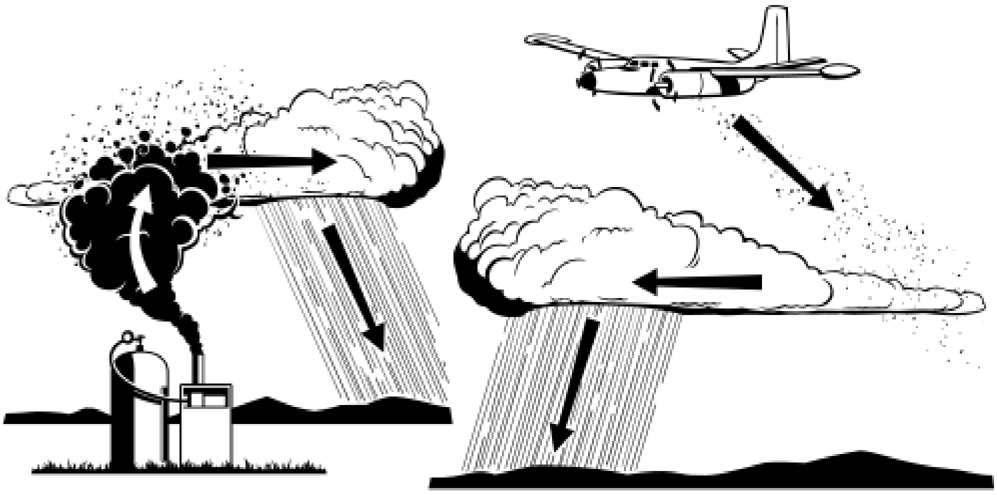
e) In various homes and offices, the culture of water management should be promoted. The use of toilets for urinating should be avoided. We should encourage the use of urinals instead of toilets, which will need to be flushed from time to time, leading to waste of water;

f) For optimal agricultural production, it is advisable to adopt crop rotation, which can assist in minimising the problem of erosion and enable farmers to cultivate other crops that demand less water during drier seasons that may be occasioned by the drought;

g) There must be promotion of the culture of recycling water by the authorities. The water used in homes and offices will pass through various drainages and move straight into the central drainage system where the water will undergo treatment and become purified and then be resupplied to the consumers. This process will help in no small measure to conserve water with the aim of preventing shortage of water presently and in future.

h) Adopting cloud seeding can also be beneficial in the mitigation of drought. Cloud seeding can be described as a method of weather modification. It is usually an "attempt to change the amount or type of precipitation that falls from clouds, by dispersing substances into the air that serve as cloud condensation or ice nuclei, which alter the microphysical processes within the cloud" (://en.wikipedia.org/wiki/Drought) (see figure 1.1). The rationale behind this method is to enhance precipitation (rain or snow). Also, the hail and fog suppression often practiced in airports can also be useful.

Figure 1.1. Cloud Seeding



Cloud seeding can be done by ground generators or by plane

Source: ://upload.wikimedia.org/wikipedia/commons/thumb/4/4c/Cloud_ Seeding .svg/500px-Cloud_Seeding.svg.png.

SELF ASSESSMENT EXERCISE

What are the safety measures in the management of drought?

4.0 CONCLUSION

In as much that it is impossible to absolutely prevent the incidence of natural threats or hazards, it is therefore imperative to educate the masses on the ways and approaches through which the effect of any natural hazard can be reduced or mitigated. The problem of desertification being experienced in most parts of northern Nigeria and elsewhere in Africa especially those countries on the Sahel belt could have been addressed to a large extent if the stakeholders had not failed in their responsibilities. The responsibility of educating the public on the management of natural hazard, manmade or any other type of threat cannot be entirely entrusted to government. The security practitioners and other stakeholders including community associations, religious institutions, corporate organisations, non-governmental organisations (NGOs) among others also have some roles to play in hazard mitigation education and coordination.

It is therefore very germane to educate the masses on various safety measures to improve their preparedness towards reducing the losses that the hazard can produce. Also, by educating the masses, various habits and actions they usually engage in, which are capable of increasing the incidence of any natural hazard can be checked by making them know the risks that such habits and actions pose to the community at large. This will definitely create an avenue for prevention of hazardous situations as much as possible.

5.0 SUMMARY

In this unit, we have discussed some of the various safety measures through which we can manage any major natural threat. We began our study by looking at those safety tips to mitigate the incidence of earthquake. Thereafter, we explained a variety of safety tips or measures to prevent or/and check such other major hazards like hurricane, flood and drought. It is my belief that this has been found to be intellectually stimulating. Thank you for your zeal and patience.

6.0 TUTORED MARKED ASSIGNMENT

Briefly discuss any five safety measures each to any two of the following natural threats: Earthquake, hurricane, flood and drought.

7.0 REFERENCES AND FURTHER READING

Hrezo, M.S., Bridgeman, P.G., & Walker, W.R. (1986). Managing Droughts through Triggering Mechanisms. *American Water Works Association Journal*. 46-51.

Walker, W.R., Hrezo, M.S., & Haley, C.J. (1991). Management of Water Resources for Drought Conditions. In: Paulson, R.W., Chase, E.B., Roberts, R.S., and Moody, D.W. *Compilers, National Water Summary 1988-89--Hydrologic Events and Floods and Droughts: U.S. Geological Survey Water-Supply*. Paper 2375. 147-156.

://en.wikipedia.org/wiki/Drought. Retrieved on 30 August, 2009.

://kashmirdivision.nic.in/Disaster_ Management/dm_center.htm). Retrieved on 28 August, 2009.

://upload.wikimedia.org/wikipedia/commons/thumb/4/4c/Cloud_ Seeding .svg/500px-Cloud_Seeding.svg.png. Retrieved on 30 August, 2009.

Error! Hyperlink reference not valid.. Retrieved on 28 August, 2009.

UNIT 2

SAFETY MEASURES IN THE MANAGEMENT OF MANMADE SECURITY THREATS I

CONTENTS

6.0 Tutored Marked Assignment
7.0 References / Further Reading

1.0. INTRODUCTION

In the previous unit, our searchlight was beamed on the various security measures to mitigate major natural threats discussed in this course or at least to reduce the losses, which their impact may have on the lives and property of the people. In this unit, we shall continue our study on the variety of safety tips to managing security threats but our focus shall shift to manmade threats. Before we go into the nitty-gritty of the study, let us quickly look at various objectives we shall strive to accomplish in this unit.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Explain safety measures against robbery;

Discuss measures to protect your vehicle from being snatched or hijacked;

Describe tips to the management of risks associated with theft; and

Clarify on which measures that can be taken to mitigate the acts of arson.

3.0 MAIN BODY

3.1 Safety Measures against Robbery

Robbery often involves the use of instruments of intimidation and coercion by a party(ies) against another party(ies) with the aim of compelling the victim party to concede his/her property in question to the offender party. Such violent instruments like gun, knife, sword, cutlass, grenade, or any other dangerous objects as the case may be, are usually used by robbers to force the victims to yield to their (robbers') demand. The danger inherent in the incidence of armed robbery often necessitates the need by every individual to be educated on the ways to reduce the effect that such hazard may have on him/her or his/her family or property. Some of the safety tips include the following:

Before the Robbery

a) Ensure that your home and office are designed in a way that passers-by or security agents can easily notice from a distance that you are experiencing robbery attack. Sadly, most banks in Nigeria often make their doors and windows either tinted or decorated with materials that make it impossible for passers-by to notice if any incident of robbery is taking place.

   It is very unfortunate that when initiating the structural design of most banks in Nigeria, little or no credence is given to security. The point we are making here is that it is rather absurd to have a structure covered with glass and the glass is tinted such that nobody can see through it to know the situation of things in the banking hall. Then, question is that if they don't wish the passers-by to see what is going-on in the banking hall, why the choice of glass rather than complete concrete blocks?

b) You should always avoid keeping large volumes of money at home or even in the office if your organisation is not a financial institution. It is also advisable that if one is a trader, one should always lodge his/her money from sales in the bank as soon as he/she makes sales worth certain amount to be determined by him/her. As security experts, we can always advise our clients in that respect as a safety tip against robbery. As you may know, if robbers know that the probability that they will not meet substantial amount of money with you is high, definitely, you will always appear to them as bad business. And thus, they will be discouraged from any attempt to rob you;

c) Installation of surveillance cameras and Closed Circuit Televisions (CCTVs) are also very useful in curbing the incidence of robbery. These security gadgets can assist us to detect the presence of robbers and alert the law enforcement agents immediately for intervention. We can also use the gadgets to monitor the movement and activities of people in and around our premises and promptly seek the intervention of the police if we suspect any persons to be potential threats to our lives and property. If we are members of the security community, we can initiate the arrest of the suspected persons for interrogation. And in the course of investigation, we find the suspects culpable, it is paramount that we step-up the investigation with the aim of arresting their co-conspirators. Thereafter, the process of prosecution should be facilitated by taking all the suspects to court;

d) Intelligence-gathering is also vital in preventing the incidence of robbery. Through intelligence, robbery attempt by criminal minds can be foiled and the suspects arrested;

e) As much as possible discourage the culture of using many entrance in your home or office. This is because the attacker or robber may sneak-in through one of the many doors unnoticed and before you know what is happening you have become entirely vulnerable to robbery attack. It is, therefore important to conduct routine check of the doors leading to your home or office as well as the inner rooms, closets, kitchen cabinets, toilets, bathrooms and other places that an enemy can hide with the intent to strike and attack you now or later.

No doubt, there have been incidents where some members of robbery gangs pretended as if they wanted to use the toilet but only aimed to have some weapons passed to them through the toilet window for robbery operation. They might have adopted that strategy because they might have foreseen that it would be difficult to smuggle in their rifles through the security door. It is therefore advisable to seal up the windows of toilets in banks but equip these toilets with air-conditioners and rechargeable lamps (that can remain on for at least one hour if there is power-cut or change in the source of power supply);

f) The use of other security instruments like metal detector, security door, x-ray machines among others are also crucial to prevention of robbery. They can detect and raise alarm of the potential threat that any identified robbery gang can pose to the organisation;

g) Always install security lights so that you can easily see anybody gaining entry into the premises and alert the security agents immediately you suspect the presence of any attacker or robber in your compound.

During Robbery

a) When a robbery is going on, make sure that you are calm because any unexpected movement can make the robber(s) infuriated. This is because such movement may be mistaken by the robber(s) for aggressive challenge from you and the robber(s) may decide to harm you in the process;

b) Carefully activate the alarm immediately you sense the presence of the robbers for police intervention;
c) If you don’t have an alarm, you can secretly call some of your neighbours or relatives for assistance like helping you to alert the public if they are staying on the same street with you, or better-still call the police and demand their prompt response;

d) You can also shorten the stay of the robber(s) by saying that a visitor is about to arrive or the community association meeting will be held in your place and it will start soon. This may make the robber(s) to hasten up and flee (://www.co-asn-rob.org/CrimeInfo/RobberyTips/during.htm);

e) It is also important to note the mannerism, speeches, dialect(s) etc of the robber(s), and watch carefully when the robber(s) is/are leaving to know the direction he/she (they) is/are taking. These information can help the police to nab the robber(s);

f) Avoid looking at the robber(s) on the face to avoid the issue of threat of personal recognition the robber(s). This is because the robber(s) will feel that by sparing your life, you can assist the police in his/her (their) arrest especially if the robbery is a very violent one;

g) You should try as much as you can to cooperate with the robber(s) and avoid acting as a hero because you may get killed in doing so;

h) If you are a security agent, act promptly to dispose of your identification card to a location the robber(s) can hardly find it. This is to hide your identity in order to avoid being killed by the robber(s). It is, therefore, advisable to always hide your ID card in the car or leave it at the office, and put it on when you are in the office or on special assignment; and

i) It is extremely unwise if you are unarmed to be aggressive towards armed robber(s). It is very advisable to lie down to avoid being hit by bullet(s) and fold your arms over your head.

After the Robbery

a) When robbery has taken place, you should call the police as soon as you notice that the robbers have left but ensure that you discretely study or take note of the discussions, attitude, mannerism, dresses and physical features of the robbers. Taking note of these features may help the police to carry out their investigation and arrest of the robbery suspects;

b) You should also make sure that you lock up the place robbed (whether home or office) with the aim of assisting the police investigators in carrying-out their work (://www.co-asn-rob.org/CrimeInfo/RobberyTips/after.htm);

c) You should also avoid discussing any issue concerning the robbery incident in public because you may not know who might be a member of the gang. On the other hand, if it is known to the robbers that you can really help the police to nab them, the gang may begin to hunt you with the intention of killing you in order to stall the investigation;

d) It is also important to cajole some of the people present when the robbery took place to serve as witnesses and be interviewed by the police. In the course of interviewing them, the police may get clues through which they can nab the robbers. However, you should note that it is wrong to coerce witnesses into making statements. In doing so, you are engaging in an action that may considered tantamount to infringement of their fundamental rights, which can rubbish the whole process of investigation; and

e) If you are approached by the media to comment on the robbery incident, you should always refer them to the police, and remain quiet and calm too.

SELF ASSESSMENT EXERCISE

Discuss safety measures to mitigate the effect of robbery.

3.2 Safety Measures against Car-Snatching or Carjacking

Car-snatching or carjacking can be described as the act of seizing and forcefully taking possession of the victim's vehicle by the crime offender through the use of dangerous weapons especially gun. Some of the safety tips to this security threat include the following:

Before the Carjacking

a) It is very important to install anti-hijack system, which is an electronic system that is usually fixed in motor vehicles to prevent car-snatchers or thieves from stealing your vehicle. The revolution in technology has also made it possible to fit an electronic monitoring device on your vehicle. These are some types of this device that can deactivate or stop the car from working;

b) Another safety tip is to have a comprehensive insurance for your vehicle. So, in the event of loss of the vehicle through carjacking or any hazard, you can easily run to your vehicle insurer for assistance according to the terms and conditions of the insurance policy. The insurer can help to get another vehicle for you;

c) Always lock the doors to your vehicle to prevent illegal entry into your vehicle by unsuspected criminals or car-snatchers;

d) Avoid making too loud the sound system in your vehicle to avoid attracting the attention of car-snatchers. This is because more often than not, the car-snatchers don't usually have a particular target in mind before setting-out for their shady business. So, don't make yourself a victim;

e) Always alight whenever the vehicle is parked, even if you are waiting for someone. It is advisable to alight to avoid being close-marked by car-snatchers; and

f) Ensure that your vehicle is parked where you can have a close watch on it, most preferably in the compound.

During Car-snatching

a) If you know that you can escape the car-snatchers, surrender the car to avoid being harmed by the criminals. As you may be aware that most car-snatchers are armed with dangerous weapons, so, it is unwise for one to allow himself get killed by car-snatchers; and

b) Be calm and if the car-snatchers ask you about the security of the car, you can tell them that there was security gadget on the vehicle before but it has been deactivated due to the stress it often put the owner into especially the way it used to cut-off ignition and the vehicle would be stationed where the problem was developed until the owner got the security company that installed it to fix the problem. You should avoid telling the car-snatchers that you are the original owner of the vehicle. By doing this, the car-snatchers may allow you to go and drive the vehicle away. By the time the security gadget will be activated, the car-snatchers will have no choice but to abandon the vehicle;

After the Car-snatching

a) You should seek medical care if you or any other persons in the vehicle are harmed;

b) Quickly inform the police about the incident and provide necessary information and details of the vehicle registration number, etc from prompt police intervention to recover the vehicle;

c) You should cooperate with the police and respond to their interrogation very effectively. Showing cooperation can be helpful in nabbing the car-snatchers by the law enforcement agents; and

d) If the vehicle is insured, you will be expected to inform the insurer to start the Claim process.

SELF ASSESSMENT EXERCISE

Explain the safety tips in managing the risks emanating from carjacking.

3.3 Security Measures against Theft

Theft can be described as a form of manmade security threat that usually involves such criminal acts that relate to illegal acquisition of another person’s property or acts of stealing like burglary, larceny, looting, fraud and embezzlement, to mention a few. Some of the safety measures to guard against the incidence of theft include the following:

Before theft

a) Putting in place security doors that are equipped with alarm in an attempt by malicious person(s) to gain entry into a facility;

b) The use of surveillance cameras and Closed Circuit Televisions (CCTVs) can also be useful in the protection of property against theft;

c) Avoid putting large sum of money at home because it can attract the attention of thieves within and outside;

d) Monitor the behaviours of the people around at home or in the office. Always suspect any secret discussions among people or abrupt end of discussion on phone when your presence is noticed by an internal person;

e) At the office, unnecessary loitering or notice of strange faces should be challenged by questioning them about their mission in your office or shop;

f) Contracting the services of security guards (whether private or public) can safeguard one's property against theft;

g) Search should be conducted on all staff irrespective of their positions or status as they come in and go out;

h) You should promote the habit of rewarding any of your people at home or in the office who makes that report a fellow involved in theft;

i) There should be severe penalty for those found guilty of theft;

j) You should also install security lights and gates to check any malicious entry into your compound; and

k) Regularly change the door locks to your home and/or office; etc.

During the incident of Theft

a) If you catch someone in the act of theft may be directly or through the use of surveillance camera or through informant, you should call the attention of few other people who can serve as witnesses;

b) If you see the act of theft going on from a distance and you notice that the culprit is about to abscond, alert the people around or the public and seek for their intervention to effect the arrest of the thief;

c) If the thief is arrested, you should ask him/her a number of questions to know if it was his/her first time of stealing your property or goods, if the offender has the support of any insider in perpetrating the act, and every other information that can assist to identify areas of vulnerability in the security of your property or goods; and

d) In case of a car theft attempt, you should alert the public and call the police immediately for intervention. You should avoid moving close to the thief because he/she may not be alone and/or may be armed with dangerous weapons;

After the Incident of Theft

a) If the culprit is arrested, avoid engaging yourself in carrying out jungle justice because the law sees such act as criminal and punishable offence. It is therefore advisable to hand over the thief to the police for further investigation and prosecution, if the suspect is culpable of the offence (theft);

b) Ensure that you give all necessary support and information to the police to aid their investigation for the eventual prosecution of the offender; and

c) Avoid discussing the proceedings of the investigation in public;

d) Avoid exaggerating the amount of money, goods or property lost to theft;

e) Fortify your security systems and infrastructure to avoid similar incident of theft in the nearest future.

SELF ASSESSMENT EXERCISE

What are the safety tips against theft?

3.4 Safety Measures against Arson

Arson can be described to mean a deliberate act of destructively setting another person's or oneself's property on fire for specific motives. Some of the safety tips to second party arson include the following:

Before the Arson

a) In as much as the event of arson remains an unexpected hazard, it is imperative for government to have relevant agencies including Fire brigades and the police to always monitor and act in mitigation of any incident of arson;

b) Enough efforts should be made to engender anger management as part of the educational curricula among various levels of learning in Nigeria. By doing this, the problem of arson will be minimal. People will learn creative ways of addressing conflict issues rather than engaging in destructive approaches to conflict management, one of these being arson. A good example is the setting on fire of the INEC office in Iddo Ekiti, resulting from alleged electoral malpractices levelled against the Electoral body by irate youths.

   There are many instances as well where students go on rampage and burn down some structures in the premises of their institutions for no other reason than resisting increase in school fees. Most times, apart from compelling them to pay the new fees, the students are also levied for the property destroyed. The question is who are the losers? Your answer to the question is the same as mine. The truth is that both the school authorities and the students are the losers. It is an indictment on the entire school system for lacking culture of dialogue and conflict transformation in the resolution of their issues of conflict. It is unfortunate that in Nigeria, most times, we wait for the upsurge of violence and destruction before we come to terms with the need to appreciate our mutual need for peaceful resolution of conflict;

c) You should educate people in your home and office on how to respond effectively when there is fire outbreak resulting from arson or any other cause. It is pertinent to identify exit routes in the event of an emergency like arson;

d) It is also advisable to install fireproof cabinets in your home and office where you can keep very vital documents and guarantee their protection in the event of fire-outbreak; and

e) It is important to install fire fighting equipment at home and office, so that when there is fire, you can fight it until the arrival of the fire brigades. This measure is helpful to mitigate the effect of arson on the structure or reduce the losses that may accompany it;

During the Incident of Arson

a) You should be calm and not let anxiety disorganise you or undermine your capacity to act reasonably to mitigate the effect of the hazard;

b) You should alert the police or any other law enforcement agent to come to the rescue;

c) You should also promptly call for the intervention of fire fighters with the aim of reducing the losses that the hazard may effect;

d) Carefully use the fire-fighting equipment available to reduce the intensity of the fire before the arrival of the fire brigades; and

e) You should locate the most secure route to exit the building as well as avoid falling into the hands of the arsonists because it may be dangerous to do so;

After the Incident of Arson

a) Assist the law enforcement with provision of vital information that will aid investigation on the cause and offenders of the crime (arson);

b) After the incident, you should begin the process of providing a report on the cause(s), suspected arsonists, dynamics of threat assessment, losses (in human and material terms) recorded as a result of the incident (incident assessment), recovery analysis and recommendations to forestall similar incident in the nearest future;

c) You are also expected to begin the reconstruction by considering vulnerabilities identified as a result of the incident and efforts should be initiated to alleviate the vulnerabilities and increase preparedness level to mitigate or prevent the reoccurrence of such incident (arson);

d) You and other victims should also undergo trauma counselling and therapeutic session to address any psychological effect that such incident may have on you; and

e) All necessary cooperation and resources should be given to the law enforcement agents in the prosecution of the offenders.

SELF ASSESSMENT EXERCISE

Explain safety measures against arson.

4.0 CONCLUSION

Appreciating the ways through which we can prevent or respond to the incidents of manmade threats is the first step towards advancing effective security management. Through proper education on safety measures to various threats to security of life and property, stakeholders can be able to improve on their preparedness and building their capacity to respond very creatively in the experience of any threats. By providing the public and our clients with safety education, we will be able to fulfill the overall objectives of our various organisations as security practitioners. The beauty of safety education also involves the opportunity of the public to act independently in reducing the impact that any threats can have on them as they will rely on us to play complementary roles in protecting their lives and property, and this will make our work easier and less stressful too.

5.0 SUMMARY

In this unit, we explored various safety tips that can be adopted to manage a number of manmade threats. We examined various steps to protect ourselves and property against the threat of robbery. Thereafter, we explained the tips to mitigate carjacking and how to reduce the losses that may be recorded as a result of its occurrence. We completed our task in the unit by highlighting the safety measures that we can appreciate to manage security risks associated with theft and arson.

6.0 TUTORED MARKED ASSIGNMENT

Discuss any five pre-incident safety tips of any two among the following threats: Robbery, carjacking, arson and theft.

7.0 REFERENCES AND FURTHER READING

://www.co-asn-rob.org/CrimeInfo/RobberyTips/after.htm. Retrieved on 2 Sept., 2009.

://www.co-asn-rob.org/CrimeInfo/RobberyTips/during.htm. Retrieved on 2 Sept., 2009.

UNIT 3

SAFETY MEASURES IN THE MANAGEMENT OF MANMADE SECURITY THREATS II

CONTENTS

1.0. INTRODUCTION

Due to the limited space and time we had in the previous unit, we were not unable to complete the overall task of discussing all the various safety measures to all the manmade threats discussed. In this unit, we shall however be focusing on safety measures to prevent or mitigate the effect of such manmade threats, which shall be our objects of study. Manmade threats are usually experienced by every society, and it is germane to develop strategies or ways through which we can reduce the losses that such threats bring about. In the next segment of this unit, we shall be exploring the objectives of this study.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Describe safety measures to undertake in the management of kidnapping;

Clarify on the relevant safety tips that can be adopted in mitigating badger game;

Identify various safety measures against extortion;

Discuss the safety measures in the management of insurgency; and

Explain measures that can be taken to ensure safety of individuals from terrorist attack.

3.0 MAIN BODY

3.1 Safety Measures against Kidnapping

Kidnapping is a security threat and criminal offence that usually involves "...the taking away or asportation of a person against the person's will, usually to hold the person in false imprisonment, a confinement without legal authority" (**Error! Hyperlink reference not valid.**). There are various ways through which we can effectively check or manage this form of security threat and some of these safety tips may include the following:

Before Kidnapping

a) To avoid being kidnapped, you are advised to reduce the things or social activities that can attract the attention of kidnappers towards you. One should not display his/her assets, nationality or institutional affiliation anyhow. For instance, a set of kidnappers may be targeting employees of a very rich company to kidnap for a ransom, if one is the type that is lousy and allows everybody to know that he/she is working in such a big organisation for the purpose of earning the respect of his/her neighbours may be la victim. The reason is that he/she can easily be a prey in the hands of kidnappers who place ransom on him/her before he/she can be released.

   As you may be aware, the security policy of some organisations absolutely does not allow the management to pay any ransom to secure the release of any staff seized by kidnappers. The rationale behind such resolution is understandable. The idea is to discourage the kidnappers from seeing the staff of the company as objects for brisk business. If ransoms are not paid, the kidnapping gang will have no choice other than to look for another work to do because kidnapping will be considered not profit-making;

b) Another safety tip that is very useful in preventing kidnapping is to make sure that you limit your movements as much as you can to avoid yourself becoming an easy prey in the hand of kidnappers. One should also avoid taking particular routes on regular basis. This is because taking particular routes regularly may afford the kidnappers ample opportunity to know where they can seize you. But, if you don’t actually have any particular routes you take all the time, it will be difficult for kidnappers to decide on a particular route to carry out their dastardly act against you;

c) If the routes from your home to office are not many, you should avoid going with the same car all the time if you have your own car. You can once in a while move around in public transport. This is because more often than not most kidnappers don’t know the actual identity of their target but use other attachments like car and house;

d) When you arrive at home, always make sure that you don’t leave your door open, and always conduct simulation in your home to identify parts of the house that can make your home vulnerable to external attack, so you can fortify your security infrastructure;

e) If you have the resources, you can install security surveillance devices like Closed Circuit Television (CCTV) at home or in the office (as an employer) to detect or/and monitor any acts of threat from enemies like kidnappers; and

f) Always get yourself and your household educated on risks generally especially as they concern lifestyles, occupation and relationships with other people. For instance, as a security practitioner, you should always enlighten your family and friends on the inherent danger associated with your job to improve their preparedness against any malicious attack.

One of the instructions you should give them is if there is a call from any stranger on issue pertaining to you, they should get in touch with you for confirmation. Your family members should not open the door for strangers without alerting you. As you may know, some criminals may decide to kidnap one of your family members to forcefully influence your decision especially when you are the officer investigating a case of crime;

During Kidnapping

a) For one's safety, it is important to show cooperation with the kidnappers to avoid being harmed, as you know, most times, kidnappers equip themselves with dangerous weapons like guns and if you struggle with them, they can get you injured or killed in the process. But, there may be some opportunity for resistance only when you feel it is safe to do so.

   For instance, you may have suspected that kidnappers are trailing you, and see them surrounding your car, as they are armed with cutlasses and knives while you are lucky to armed be with gun. Then, you can use the gun to negotiate your escape but after the escape you may find it difficult to deduce the motive of the assailants. Therefore, you need to tighten your security and make your security infrastructure more fortified;

b) If you have been overwhelmed by the attack from the kidnappers, avoid engaging them in hot argument but rather you should be calm. You should avoid noticeable eye contact with the kidnappers because they can mistake it for aggression;

c) If you have already been seized by the kidnappers, don't allow fear and shock that characterise the attack to weigh you down. You should, therefore, make yourself active by tasking your security intellect in devising ways through which you can be on top of the situation like plotting relevant tactics for escape. You are strongly advised to facilitate your own escape only when you find the option necessary and safe too;

d) The kidnappers will intimidate you but you should remain calm and never believe most things they tell you. Sometimes, kidnappers engage in discussion basically with the aim of making you sympathetic and supportive to their cause, you should ensure that you don't develop Stockholm syndrome in the process. Stockholm syndrome involves developing sympathy for the kidnappers and their objectives;

e) You should also study the attitudes, discussions, dressing, motives, mannerisms etc of the kidnappers through your mind and avoid writing down anything on paper as memoir. This is because if you are caught in the act of writing notes, the kidnappers may get infuriated and decide to injure or even kill you;

f) You should also agree with the kidnappers if you are asked to talk on phone, video, or even radio, and absolutely restrict yourself to what you are asked to say;

g) Avoid sharing clothes with the kidnappers, so that you will not be mistaken for the kidnappers in the event of rescue attempt. As you may be aware, the rescue team would have done some underground work like seeking to know the cloth you wore on the day you were kidnapped so that they would not mistake you for any kidnapper. May be in the course of rescuing you, the kidnappers may engage the rescue team in a gun battle, and if you share cloths with the kidnappers, you may be mistaken as one of them; and

h) Similarly, if you see that there is a gun battle between the kidnappers and the rescue team, you are advised to lie on the floor and put your hands on your head to avoid being hit by bullet(s). The reason, you are advised to put your hands on your head, is to show that you are not armed and not constituting any threat, so that you will not mistakenly be shot by the rescue team some of whom may not know you personally;

After Kidnapping

a) If your release is secured through the payment of ransom by your relatives or the management of your organisation or through the use of force or escape, you are expected to assist the law enforcement authorities to nab the culprits so as to reduce the incidence of kidnapping. It is, therefore, important to cooperate by giving enough details about the incident to aid investigation; and

b) You should also appreciate the offer of post trauma counselling.

SELF ASSESSMENT EXERCISE

What measures can you proffer for safety against kidnapping?

3.2 Safety Measures against Badger Game

Badger Game is a form of security threat can involve using tricks or simply to set up somebody with the aim of influencing his/her decision in the discharge of his/her duties with the instrument of blackmail. Owing to the risk that this threat portends to the capacity of any individuals to carry out their official duties without fear and favour, it is imperative to provide some of the measures that can help one to safeguard the ethics of practice without succumbing to cheap blackmail aimed at making one to work against his/her conscience. The safety tips include the following:

Before the incident of Badger Game

a) You should ensure that you are very careful in the selection of those with whom you will have relationship or friendship and classify such relationship according to the trust you have for each individual;

b) Avoid regular night-outing;

c) Educate your family on the risks involved in your chosen profession in order to enlighten them against actions that can jeopardise your career;

d) Avoid engaging in any acts that you will not like to come to the knowledge of the public; and

e) Always operate open door policy and discourage habits of divide and rule or malicious talks among your colleagues.

During the Incident of Badger Game

a) Be calm in order to be on top of the situation;

b) Seek adequate information as regards the objectives of the enemies or blackmailers and the identities of virtually all parties involved;

c) Promise them of cooperation with the aim of deceiving them, so that you will have an opportunity of paying them back in their own coin;

d) The use of portable tape and secret cameras can also be useful in recording your conversations and meetings with them; and

e) As the case may be, look for reliable top executive in the Press or any other media outfits, to cover the meetings and conversations between you and the culprits secretly and ensure that the event is circulated by the Press. This will also allow the public to know that the entire event was a set-up to put your reputation in disrepute and to influence your decision and force you to act against your conscience in the discharge of your duties.

After the Incident of Badger Game

a) If you know that the action you have engaged in can undermine the credibility of your office, it is appropriate to resign your appointment;

b) Report the case officially to the management and narrate the incident from beginning to the end, and apologise for falling into the trap of the enemy(ies). You should also give the names of all the personalities behind the drama (the names of the culprits you can identify); and

c) If the case involves police intervention, try as much as possible to cooperate with the police and get yourself a lawyer who will guide you legally in the course of trial.

SELF ASSESSMENT EXERCISE

What are safety measures in the management of badger game?

3.3 Safety Measures against Extortions

Extortion can be described as a criminal act or security threat, which involves "…..making illicit funds from organized crime such as illegal gaming, prostitution rings, money laundering, smuggling etc...and obstruction of justice (when it pertains to mafia figures) is usually threatening someone not to testify or attempting to buy judges or jurors or key witnesses thus impeding the process of the justice system" (://answers.yahoo.com/question/index?qid=20090909052116AAdrVS9). There are several measures through which you can safeguard yourself and property against extortion, and these include:

Before the Incident of Extortion

a) Avoid carrying large expensive jewellery, too many credit cards or ATMs or any other important valuables about. It is better to such things at home;

b) You should avoid accepting ride from strangers;

c) Avoid travelling alone in a private vehicle;

d) Ensure that all your vehicle particulars are with you;

e) Avoid carrying any goods that you cannot provide receipts for;

f) If you are travelling to an unfamiliar place with your car, make efforts to seek information about traffic rules, culture and risks peculiar to the place;

g) You should avoid making known your socio-economic status in an unfamiliar land or place;

h) Do not accept bags or other items from a stranger;

i) Do not give your bags to a stranger to carry for you;

j) Avoid night-outing in a strange land;

k) Ensure that you obey traffic rules and regulation;

l) Avoid doing business with anybody who you don't know much about his/her business activities or dealings; and

m) Always be security-conscious and avoid getting intoxicated from excessive intake of alcohol; etc.

During the Incident of Extortion

a) Feel composed and calm. Do not fidget because the extortionists may take advantage of the situation;

b) If the extortionist is a law enforcement agent, note his/her name, badge number, patrol vehicle number and the time the crime (extortion) is being perpetrated against you;

c) If they threaten you with arrest, do not resist the arrest and demand for where their station is located;

d) Tell them that you will like to inform your relatives and friends so that they will know where to find you; and

e) You can secretly send a short message to a friend and a relative about your plight intimating them about the location, time, and details of the law enforcement agent(s) wishing to extort you for prompt action;

After the Incident of Extortion

a) Report the case to the law enforcement agents if the extortionists are civilians;

b) Where the extortionists are law enforcement agents, report the case to their superior officers for disciplinary actions to be taken against them; and

c) In a situation where you feel that nothing is being done by the law enforcement authorities to punish the offenders, you can approach the court for redress; etc

SELF ASSESSMENT EXERCISE

What safety measures can you can take against extortion?

3.4 Safety Measures against Insurgency

Insurgency usually involves an armed struggle or rebellion aimed to challenge the sovereign power of a constituted authority. There are several safety measures in the management of insurgency, some of which include the following:

Before the Insurgency

a) The culture of cultural relativism should be promoted while attitude of ethnocentrism should be discouraged in order to foster peace among people across various cultural boundaries;

b) People should be educated on intercultural dialogue and communication to subdue any negative emotions, which can provoke a situation of intercultural hatred and enmity;

c) We should always admonish the government on the need to advance good governance and nation-building;

d) We should always participate in the democratic process by regularly voting for candidates of our choice and law enforcement agents should endeavour to be absolutely neutral and unbiased in the maintenance of law and order during the election;

e) The security sector should realise that it derives its authority from the people and will need to avoid being used by the political elite to repress or oppress the people;

f) All stakeholders should ensure that the independence of judiciary is always safeguarded;

g) The use of violence to actualise political objectives or any other objectives should be entirely discouraged while peaceful resolution of conflict should be encouraged at all levels of human relations;

h) The issue of official corruption and other forms of corruption should attract very grave penalty like long jail terms without any option of fine;

i) There should be effective intelligence system that encourages active participation of the public in intelligence-gathering activities;

j) Any gathering of people, which one feels can pose a security threat to the society at large should be promptly reported to the law enforcement agents; and

k) There must be rule of law and respect to the fundamental rights of the people must be guaranteed; etc

During Insurgency

a) You should inform the government of the presence of any insurgents in your neighbourhood. In doing this, you should avoid making your identity known;

b) If you notice that the insurgents are on an offensive mission, you are advised to run for cover;

c) And if you feel that it is unsafe to continue staying in your present location, you can decide to evacuate yourself, family and important property including vital documents and relocate to another place where your security can be guaranteed;

d) If you are found among the victims held hostage by the insurgents, be calm and avoid acting like a hero to avoid being killed by the insurgents. You are therefore advised to cooperate with them and pretend as if you support their cause;

e) If the insurgency is based on inter-ethnic aggression, it is better you undertake evacuation without wasting time to other places where security can be guaranteed;

f) You can seek alternative shelter in the military barracks or other relation's house where there is less or no absence of the insurgents;

g) Always create escape routes at home and in the office where you can easily negotiate your escape in the time of emergency that may be occasioned by attack from the insurgent;

h) You should join the movement of anti-war activists and enjoin others to join as well, with the aim of articulating for peaceful approaches to the resolution of conflict rather than the use of violence. One revelation is that, some military men and officers now identify themselves with peace movement especially owing to the fact that virtually all wars are finally laid to rest on the conference table rather than the battle fields; and

i) Try as much as possible to cooperate with government forces to expose the hiding places of the insurgents you know; etc.

After the Insurgency

a) The insurgents should be disarmed, demobilised and integrated into normal life while the civilians forcefully conscripted by the insurgents should be rehabilitated and reinstalled to civilian life;

b) There should be post conflict-reconstruction like rebuilding of social infrastructure destroyed as a result of war or violence, etc;

c) There should be post conflict peace-building through which wounds of war or violence can be healed for genuine reconciliation and actualisation of positive peace; and

d) A truth and reconciliation commission should be set up to provide avenue for the victims and offenders of war crimes to express their minds and experiences and the challenges they face in their individual lives. In the course of doing this, the offenders will be made to feel sober and accountable for the atrocities perpetrated against victims while the victims derive ultimate joy in finding space in their hearts to forgive the offenders. The ability of the victims to forgive their offenders remains a subject of debate among peace and conflict theorists.

SELF ASSESSMENT EXERCISE

What are the safety measures to managing insurgency?

3.5 Safety Measures against Terrorism

Terrorism can be defined as a systematic and ferocious use of violence, a form of guerrilla alternative to conventional warfare by state or non-state actors, with the strategic creation of psychic fear and (or) tactical production and reproduction of wanton destruction in epochal dimension purposely in realizing political objectives or ordinary public attention or both variables. Some of the safety measures to terrorism include the following:

Before a Terrorist Attack

a) It is important to be alert and take a good watch of the surrounding area and quickly respond when you see some suspicious people that you consider pose a threat by immediately informing the law enforcement agents;

b) Whenever you are embarking on a journey avoid picking strangers on the road;

c) Anytime you receive a threat call, always try to be calm and record the conversation with the suspected terrorist calling provided that your phone has the function to record voice calls. You should quickly inform the law enforcement agents about the threat you have received from the caller. If you recorded the conversation, copy it in a tape and give it to the police or private investigator(s) for further action;

d) Also when travelling locally or internationally, always avoid accepting packages that you are not sure of their contents from people especially strangers, not for any amount. The reason is that the cost of damage that you may suffer for accepting such packages may be far higher than what you are paid. Therefore, it is necessary to be careful in dealing with people;

e) At home or in the office, you should ensure that emergency routes are created, which can facilitate smoother evacuation in the time of emergency situations that may be occasioned by terrorist attack; and

f) Installation of surveillance camera and Closed Circuit Televisions can also be useful to prevent the incidence of terrorist attack(s). Through monitoring and surveillance, any gang of terrorists can be rounded-up by the law enforcement agents during the time they are planning to carry out their dastardly act;

During a Terrorist Attack

a) In the event of a terrorist attack, you should be calm and avoid anxiety because anxiety can deprive you the opportunity to respond creatively and effectively to mitigate the impact of the hazard on you;

b) Quickly inform the law enforcement agents of the terrorist attack and notify them of the emergency response that the situation requires. You should give details of the location and other relevant information that can help in facilitating a prompt and effective intervention. The challenge that people face in this part of the world is that the response of law enforcement agents to terrorist events is rather too lackadaisical and not timely too. Some of the factors responsible may include poor preparedness, lack of adequate working tools, operational deficiency, lack of hazard mitigation practices, official incompetency, among others;

c) Carefully locate the emergency routes through which you can negotiate your escape from the building under a terrorist attack;

d) If you are in a high-rise building, it is advisable to avoid using the lift because it is possible that the terrorists would have anticipated that many of the occupants will rush to the lift to escape from the building. In this case, it is very likely that the terrorists would plant an explosive or dangerous gas in the lift by which many people will lose their lives. It is therefore wise to carefully use the stairs and don’t panic to avoid stampeding;

e) As you are escaping from the building you need to exercise caution. As you are approaching the door, you are advised to feel the lower, middle and upper parts of the door with your palm or forearm to know if the door is hot or not. In a situation where you find the door to be hot, please seek alternative route because of the inherent danger in opening such a door. But, if the door is not hot, then you can slowly open it to negotiate your escape;

f) In a situation where the terrorists are shooting sporadically, you should lie on the floor and crawl as you locate the escape routes;

g) If the terrorists are everywhere and there are many already being shot dead by the terrorists, you can put one of the dead bodies on top of yourself in a way that will not be suspicious to the terrorists and pretend as if you are dead and study the movement, conversations and dresses (if possible) of the terrorists. You should maintain your position as the terrorist event lasts.

After a Terrorist Attack

a) Rescue efforts should commence immediately wasting to rescue the victims of the terrorist attack,

b) If a victim is covered by debris, he/she should use an handkerchief or clothing to cover his/her mouth;

c) If a victim is trapped and it is noticed that rescue efforts are on, he/she should knock on a pipe or wall to alert the rescuers that he/she is there. You can also shout so that the rescuers will know that you are there;

d) There is the need to use masks by the rescuers to avoid any form of chemical or biological attack from the hazard;

e) Due to the fact that biological agents are not usually detected immediately, it is incumbent on government to find out through its intelligence network and crop of scientists if there was any use of biological weapons by the terrorists. And if it is detected that biological weapons were used, efforts should be made to quarantine the location and take all the victims to the hospital for diagnosis and comprehensive treatment;

f) The victims should also undergo a post trauma counselling;

g) Structural engineers and other building engineers should also examine the affected building to know if its foundation has been weakened as result of the terrorist attack; and

h) Where the foundation of the affected building is confirmed weakened by the building expert, the building should be pulled down to prevent avoidable deaths that the eventual collapse of the building may cause; etc.

SELF ASSESSMENT EXERCISE

Write a brief note on the ways through which we can advance our safety against terrorist attacks.

4.0 CONCLUSION

Educating people and members of the security sector on security tips in the management of manmade threats is very crucial in the effective management of security in any given society. As security experts, it is paramount to cultivate the habit of popularising among people or our clients as security expert on ways through which they can safeguard their lives and property against any manmade threat. In doing this, we are on the pedestal of building the capacity of the public or our clients towards acting proactively in the event of threat to reduce the effect that such threat can have on their general wellbeing.

5.0 SUMMARY

In this unit, we have succeeded in identifying and explaining various safety measures that can be applied and adopted to managing some manmade security threats. We began our study of the variety of safety tips by looking at those measures that can be used to mitigate kidnapping, and thereafter we explained the safety guidelines to other threats including badger game, extortion, insurgency and finally terrorism. I have no doubt that you have found this unit thought-provoking and interesting. Thank you for your patience and quest for knowledge. If you have any question regarding any aspect of this unit, you are advised to get in touch with your instructional and tutorial facilitator or the course coordinator as the case may be. Good luck.

6.0 TUTORED MARKED ASSIGNMENT

Discuss any five safety measures to any two threats among the following manmade threats: Kidnapping, badger game, extortion, insurgency and terrorism

7.0 REFERENCES AND FURTHER READING

://answers.yahoo.com/question/index?qid=20090909052116AAdrVS9. Retrieved on 31 August, 2009.

Error! Hyperlink reference not valid.. 31 August, 2009.

UNIT 4

CIVIL SECURITY: MEANING AND APPROACHES I

CONTENTS

1.0 INTRODUCTION

The issue of security has been very germane to the peaceful cohabitation of people in any given community or state. Security involves several activities that are interconnected to the overall maintenance of law and order in any given society. The ultimate goal of security is to protect the lives and property of the people, and this corroborates the need to co-opt the public in the security activities and planning (see ://portalnano.ru/files/20). Therefore, it is a truism to extend the participation and decision-making processes to the people in order to achieve the overall objectives of securitisation.

As a matter of fact civil security appears to be the ultimate solution to security problems that may pervade any society. This is because with the desire to protect the lives and property of the people against any natural and man-made attacks or threats, it is more pertinent to build the capacity of the public to respond very appropriately and effectively too, to hazardous events and security attacks such as organised crime, terrorism among others, by engaging in actions that can reduce losses from such hazard or security threats.

In this unit, we shall be discussing the meaning of civil security as well as other areas of discourse pertaining to it. Due to limited space in this unit, we shall focus only on risk education and its elements in examining the various approaches to civil security, and we shall employ the task of explaining other approaches in the subsequent unit. Meanwhile, in the next segment of this unit, we shall browse through the various tasks we shall undertake on the subject in the objectives of the unit. I have no doubt that you will find this unit very interesting and intellectually stimulating.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Define civil security;

Outline various approaches to civil security; and

Explain risk education as an approach to civil security and its elements.

3.0 MAIN BODY

3.1 Meaning of Civil Security

The experience of the world in recent time has shown that security has evolved to a new stage where the importance of the civil population to security management cannot be underestimated. There has been a shift in security threat discourse where major attacks and threats come from non-state actors (see ://www.bmbf.de/en/6293.php). In this case a handful of criminals may form a group to terrorise a whole nation thereby posing greater threat to the general security atmosphere even beyond national boundary. For instance, a group like the Al-Qaeda network poses a greater security risk to the most powerful nation on earth (the US) than any of its rival states like China and Russia. If security involves initiatives, which must also "focus on the impact of natural disasters or major accidents and the restriction of damage" (://www.bmbf.de/en/6293.php), it is therefore imperative to adopt civil security framework, which will enhance the capacity of the public to act on their own in times of emergency and hazardous events.

How do you describe civil security? Civil security can be described as any conscious measure taken by stakeholders aimed at reducing vulnerability to the security of the public by enhancing the capacity of individuals to mitigate danger and security threats, as well as recovering from any form of security attacks whether they be natural (like hurricane, tornadoes, earth quake, tsunami etc), or considered to be man-made (arson, robbery, blackmail, etc). Civil security is so crucial because it "provides an outlet for individual participation in and contribution to homeland security" (Dory, 2003b). The growing relevance of involving civil population in security practice has is very evident in the contemporary world. This view was supported by President John F. Kennedy several decades ago, at the height of the nuclear threat episode between the East led by the defunct Soviet Union and the West bloc led by the United States. According to him:

To recognize the possibilities of nuclear war in the missile age, without our citizens knowing what they should do and where they should go if bombs begin to fall, would be a failure of responsibility (Kennedy, 1961).

Considering the foregoing, you may agree with me that the essence of civil security is to redefine the traditional security system and present a new paradigm in security discourse such that attention is now geared towards building the capacity of the civilians in responding to hazards and security threats. The need to educate the masses on various aspects of security cannot be over-emphasized because the goal of security will be defeated if the main stakeholders (the people) remain vulnerable to attacks and are helpless in taking care of themselves in the event of security threat.

Shalamanov *et al*. (2005) present different perspectives to the definition of civil security and according to them civil security can form the following:

(a) Better interdepartmental coordination. If properly implemented, the broad interpretation of the Law on Crisis Management will lead to the establishment

of a civil security system that is legally described as National System for Crisis Response. In this respect, the role of the National Crisis Management Center is crucial.

(b) Active civil society participation in the provision of security. The active civil participation is the connecting link between "traditional" civil protection and civil security. Nowadays security cannot be provided by the state itself. The engagement of civil society becomes indispensable. Civil society structures, NGOs, voluntary local formations as well as business organizations and the scientific community are the potential resource for the establishment of a third pillar of the security sector;

(c) Good governance and effective democratic civil control over the security sector. Participation is the best opportunity for proactive control;

(d) New strategic culture of civil society. The establishment of a civil security element of the security sector is a challenge to the maturity of civil society. The ability of civil society to fill in the vacuum left by the diminishing traditional state fast before organized crime is vital.

SELF ASSESSMENT EXERCISE

How would you describe the concept of civil security?

3.2 Approaches to Civil Security:

In this segment, we shall simply list the four basic approaches to civil security to make judicious use of space. These approaches shall be extensively discussed subsequently. They include the following:

a) Risk education;

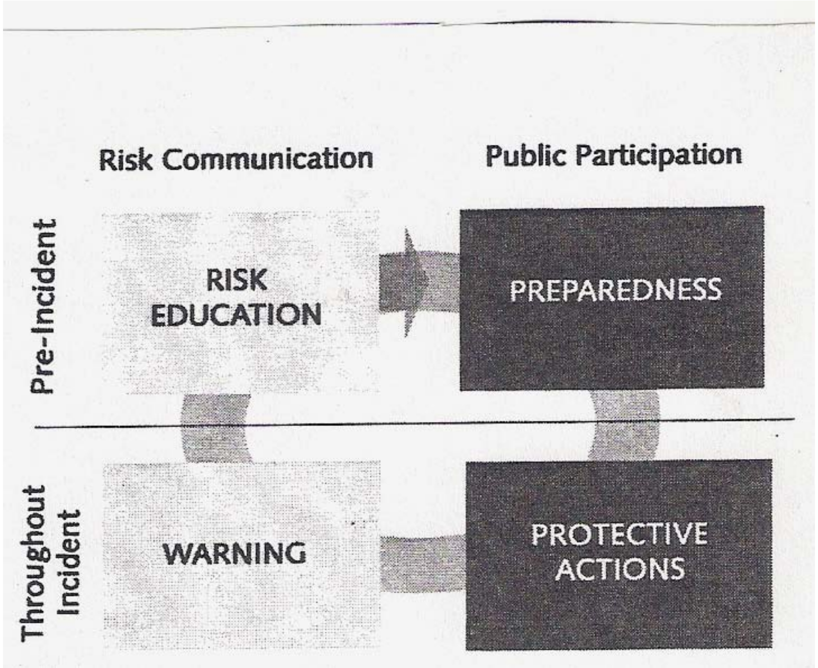
b) Preparedness;

c) (Public) Warning; and

d) Protective Actions

Civil security involves a network of activities which demands connecting various approaches that are brought to bear at different levels of security management. In security planning and management, we are often familiar with two environments: **pre-incident** (pre-hazard or attack) and **throughout incident** (post hazard and attack). The through incident environment features various activities of intervention during the incident of security threat and its aftermath, please see figure 1.1.

Figure 1.1 Integrated Civil Security Approaches



Source: Dory, A.J. (2003a). *Civil Security: Americans and the Challenges of Homeland Security*. Washington DC: CSIS.

Civil security involves drawing a framework that presents us with diverse strategic initiatives and activities that enable the public to have adequate knowledge of incidence of risk through the process of risk education in the pre incident stage. The security sector mostly performs this function by communicating (risk communication) with the public through several forums and platforms like the web, television, radio, newsletter, among others.

Having being educated on the risks that underlie potential security threats or attacks, people can then be prepared against such threats. In a situation whereby a security threat occurs, the security sector communicates with the public and issue warnings by alerting or notifying them of the occurrence of a hazard, and the steps they should take to forestall disaster that may result in huge loss of lives and property, as part of protective actions.

Also, in a situation whereby a hazard or attack occurs, the security sector communicates with the public, warning them through alert and notification about the security threat happening or about to occur. Thereafter, the public needs to be given additional (professional) advice on steps to take to reduce losses and or be assisted with further necessary protective actions, to reduce the effect of the attack or hazard on the wellbeing of the public. For instance, if there is an outbreak of bird flu infection in a community, the government may reasonably decide to quarantine or restrict everybody coming from such community to another community until essential medical tests have been performed on the affected people to know their health status before allowing them into another community. This protective action is taken to reduce the spread of the disease, which is considered capable of undermining the health security of the public. In the next unit, we shall begin our analytical task of the various approaches to civil security by discussing risk education and its elements.

SELF ASSESSMENT EXERCISE

List various approaches to civil security.

3.3 **Risk education**

From time immemorial, risk has been part of human life. Risk that pervaded the Hobessian state of nature resulting from insecurity embedded in that situation where no Sovereign power existed to regulate the affairs of men, mandated the people to surrender their individual sovereign rights to a central Sovereign authority (government). Meanwhile, that contractual agreement brought unto people another risk- the possibility of the emergent Sovereign power to fail in meeting the expectations of the people or its failure to perform well its functions or involve in oppressive and repressive actions against the people as argued by J.J. Rousseau.

The foregoing is illuminated by Holton (2004) who argues that there are two issues that determine the existence of risk. The first is uncertainty about the potential outcomes from an experiment. The second issue focuses on how material the outcomes in providing utility are. Thomas Hobbes contended that people resolved to take the risk of surrendering their sovereign power to a central Sovereign entity because of the brutish and nasty nature of Hobessian state. Though, uncertain of whether their lots would be better or not under the new arrangement, but due to perpetual absence of security of lives and property that existed prior to convocation of sovereign political authority a state, they still found it a good idea to concede their individual sovereignty to a central authority, which they believed could provide them safety and guarantee their wellbeing.

Here, despite the uncertainty, people still believed that it was better to take a risk in the convocation of a new Sovereign power than perpetuating themselves in the risk that triggered the lawlessness and disorder that characterised the state of nature as presented by Hobbes. The anticipation of the people was that the potential outcomes would provide utility. This can be said to mean that people hoped that their action would help them to have a new situation through which their safety and security of their lives and properties could be safeguarded by the Sovereign authority.

At this point, it is pertinent to look at some of the existing definitions of the term risk for our better appreciation of the subject. Well, according to Niklas Luhmann, risk can be defined as:

….the threat or probability that an action or event will adversely or beneficially affect an organisation's ability to achieve its objectives (Luhmann, 1996).

Some of the other definitions of risk may include the following:

Risk is the probability that a hazard will turn into a disaster. Vulnerability and hazards are not dangerous, taken separately. But if they come together, they become a risk or, in other words, the probability that a disaster will happen (://www.unisdr.org/eng/public_aware/world_camp/2004/booklet-eng /Pagina 9ing .pdf).

Risk is a concept that denotes the precise probability of specific eventualities. Technically, the notion of risk is independent from the notion of value and, as such, eventualities may have both beneficial and adverse consequences. However, in general usage the convention is to focus only on potential negative impact to some characteristic of value that may arise from a future event (**Error! Hyperlink reference not valid.**.).

From the above definitions, one thing that comes to our mind is that risk may be summarised as uncertainty in the outcomes of events or actions. Risk colours every aspect of human activities and relations because of the possibility that the outcomes may be partially or absolutely in variance with our expectations. A good example is a case of a retiree, who due to the unpredictable economic climate of Nigeria and not wanting to risk investing in just any business, decides to use his/her gratuity to build a house with the aim of letting out it to make money. His/her desire is to use the money from the property to take care of his/her needs and for the security of life after service, so that he/she can still have something to fall back on, even when pension is not (promptly) paid.

Here, we may see ingenuity in this retiree’s idea considering the plights of pensioners in Nigeria who are always maltreated by successive governments, but such a plan is not also devoid of risk. Let us put it this way, after the retiree in question has let out the house, one of the tenants through his/her carelessness left a lit candle on the table and in the twinkle of an eye, the house was engulfed in flames. Then, the question that would likely come to our minds is- how can the retiree get back his lost fortunes?

Nonetheless, this scenario underscores the importance of getting sufficient risk education in carrying out specific activities and undertaking a particular project or the other. Mandating the careless tenant to build another house for the poor retiree may be a fruitless effort especially when he/she does not have financial capacity to do such. Even if taken to court, little can be done to prevail on the careless tenant except he/she the means to provide the landlord-retiree with another house. Above all, the action of the tenant may not be considered as arson because the damage was not intentional but he/she may be penalised for being careless.

In the worse-case scenario, if the offender (the careless tenant) dies in the inferno, what will be the fate of the landlord-retiree? Your answer is the same as mine- total loss on the part of the landlord. Meanwhile, if there was adequate risk education on the part of the landlord-retiree he/she would have taken steps to avoid such loss and the steps may include insuring the property and equipping the house with fire-fighting facilities like fire extinguisher. Availability of fire-fighting equipments will help in mitigating or reducing the losses resulting from incident of inferno. There is no doubt that educating people on risk is very essential in providing them opportunities for safety in their businesses, activities, and the overall security of their lives and property.

Risk education and communication is a fundamental element of civil security. It is the foundation of civil security (Dory, 2003a: vi). As you may be aware, risk adorns every aspect of the life of man. A man and woman go into a relationship but only hope that things will work out fine for them. In some situations, courtship may lead to marriage while among some lovers the relationships will fail due to one reason or the other. Even where the relationship leads to marriage, some unexpected circumstances may come up, which can have adverse effects on the marriage.

For instance, in the beginning, a couple may love each other very dearly but if the marriage is not blessed with babies, the couple may decide to search for solutions, and in the process, the security of the marriage may begin to be threatened if no legitimate solutions seem to work in their favour. Thereafter, arguments and counter-arguments as well as accusations and counter-accusations may ensue that may lead to the eventual collapse of the marriage. This, in no doubt, shows the existence of risk in the relationship not only between man and woman but among people in general. According to Weyman and Shearn (2004: 6), the objectives of risk education can be summarised into three, which include the following:

(a) Awareness raising - strategies designed to disseminate knowledge and understanding of sources of harm;

(b) Transferable skills - progressive approaches that aim to develop transferable life skills (relating to the risk assessment and control); and

(c) Behaviour modification - approaches that aim to reduce risk taking behaviour.

We do certain things sometimes without having absolute control over their outcomes, yet we still take the risk in undertaking them. Even, where we have absolute control over the events, it is possible for some things to crop-up to change the course of the events, which may make the outcomes of such events short of our expectations.

SELF ASSESSMENT EXERCISE

How do you describe risk education as an approach to civil security?

3.31 Elements of Risk Education

a) <u>Development of unclassified national intelligence</u>: There is the need for government to create mechanisms aimed at developing unclassified national intelligence estimate on various threats to security i.e banditry, all forms of terrorism, ethno-religious violence, to mention a few. It is very ridiculous that various intelligence agencies have continued to play down the inherent risk involved in the way the political leadership in Nigeria continually plunders the resources of the nation with impunity. If the political office holders are educated on the risks such as political turbulence, increasing criminality, violence, and other negativities, the nation is exposed to, due to the growing incidence of corruption that pervades Nigeria, many of these government officials may have a rethink to continue to steal public funds.

The fact is that they themselves as culprits will also be victims of their own undoing. A good example is the problem of incessant political assassination where some political elites contract some of those (masses) they oppress to kill their fellow political actors for one political objective or the other. This development corroborates the adage of the *Yoruba* people of south-west Nigeria, which says that ‘a bird perches on the rope, the rope is unsteady while the bird itself that is on the rope is uneasy’.

It is important for intelligence agencies to educate political actors on the implications of their policies especially the risk such policies may pose to the overall security of the nation. For instance, in the Niger Delta, many of the political elites in and outside the region have been accused of using the vulnerable youths as party thugs armed with weapons like guns, cutlasses among others, to win elections and in the aftermath of elections, these youths are abandoned by their former patrons with no efforts by these politicians to retrieve the weapons from their thugs.

Unfortunately, these youths, after being abandoned by their former masters became frustrated, and begin to devise means for themselves to survive especially when they have understood the dynamics of economics of violence. So, many of them become armed robbers, kidnappers, saboteurs, to mention a few. The elites and their relations now become the main targets of kidnappers, a situation, which speaks volumes of the risk inherent in attitudes of maladministration and corruption;

b) Scenario-building in risk education: Enough efforts should be made in building scenarios to educate the public on risk, so that they can understand the nature and degree of possible security threats. It is very unfortunate, in Nigeria, despite the existence of various regulatory, security and intelligence agencies, that the citizens are continually exposed to different avoidable threats. For instance, the damage done by ‘wonder banks’ could have been prevented if the Central Bank of Nigeria (CBN) lived to its responsibility not only by preventing such clandestine institutions from operating but also providing adequate education to the public on the risk involved in transacting business with such fraudulent institutions.

Sadly, it took the CBN more than two years of the existence of such financial institutions before it could advise the public on the inherent danger in transacting business with those institutions. It is more pathetic that those institutions were registered by the government without considering the risks underlying their operations. The public intelligence officials that are supposed to provide guidance to government and public on how the activities of these wonder banks posed a great risk to the security of the public failed in discharging their duties in this respect, while it is laughable that many of them were also found patronizing those clandestine financial institutions due to their thirst for making quick money;

c) Interactiveness in risk education: It is imperative to make risk education interactive, so that the process will be participatory. In this case, the government should provide various forums through which individuals and respective security agencies can meet to discuss and brain storm as well as enlighten one another on different threats while appreciating the risks such threats pose to the security management of their communities. These forums may include town hall meetings, radio or television programmes and web casts, to mention a few. The importance of creating interactive platforms in risk education cannot be over-emphasized. For instance Nigeria Police has adopted the strategy of shortening the distance between her and the public through its community relations;

Gladly, police officers now have meetings with the people in communities, especially to educate the masses on the risks involved in their attitudes to security and to assist them in understanding possible threats to security of the community at large. For instance, in many communities, people are ignorant of the risk of mounting high fences around their houses for security reason. For instance, if someone is being robbed, how can passers-by know that he/she is in distress? Whereas, if it is a low fence, some of the neighbours may detect and call the Police for rescue. The same ignorance applies to the neighbourhoods blanketed by fortified gates, which denies security rescue teams i.e. Police to gain easy access in situation(s) of distress;

d) Massification of Risk education: Much emphasis should be placed on educating the general public on security risks. Risk education should be incorporated into the school curriculum from primary level to tertiary level. It should be taught in places of worship, community associations, work places, professional organizations among others; and

e) Active Participation of individuals in risk education: individuals should endeavour to participate actively in the process of risk education such as attending police-community meetings, seeking for information from relevant security agencies whenever the need arises, and exploring other interactive forums like asking questions on any aspect of security that desire to have knowledge of by participating on security talk show especially when relevant security experts are invited on the radio or television. But, it is worthy to note that, not every security information can be shared with the public.

It is, therefore incumbent on the concerned security officers either public or private to enlighten the public on the importance of keeping such information secret. Take for instance, if a Police chief is on a radio programme, and a caller seeks to inquire from him/her on the number of ammunitions each Police man/officer on patrol can have, it will be highly unethical for such a Police chief to disclose such information because of its capability to undermine the overall operation of the Police in security management.

However, an experienced security officer will educate the caller and general public on the risk in disclosing such information not only to the security of the Police personnel but also the general public. Responding creatively to questions by security officers will allow security agencies to enjoy increasing confidence from the public, which will aid the active participation of the public in security management.

SELF ASSESSMENT EXERCISE

What is Risk Education?
Explain any four elements of risk education?

4.0 CONCLUSION

Civil security can be described as any conscious measure, taken by stakeholders with the aim of reducing and addressing vulnerability to their security. It helps to educate people on risks pertaining to any potential security threats or hazards and enhance their capacity to prepare against any potential threats. This will afford them the opportunity to respond effectively on their own without waiting for intervention from emergency or law-enforcement agents, as a way to reduce losses or the impact of the attack or hazard on their lives or/and property.

There is no doubt that modern securitisation departs gradually from the traditional approach of security that entirely alienated the civil society or civilians to play active roles in security planning and management. This instructs the concept of community policing that has been articulated by the police authorities in the country but in practice, Nigeria still has a long way to go compared to European countries. One of the reasons is poor implementation of the programme, and another factor responsible for the poor credential of community policing in the country can be blamed on the negative perception people still have towards the police resulting from the nefarious activities of most of its personnel and lack of regard for the public. Against this background, Nigeria police needs to undergo serious reforms to show to the world that it is not only effective but also independent in discharging its functions. This law-enforcement agency has continued to be accused of being an instrument in the hands of some politicians to rig elections and repress the public it is supposed to serve.

5.0 SUMMARY

In this unit, we began our academic journey by examining the meaning of civil security looking at some of the existing definitions of the concept. Though, the concept is new in security studies and practice but more scholars are gradually attracted to conduct research on this new concept of basic security. We continued our study by highlighting various approaches to civil security. Thereafter, we shed light on the meaning of risk education as one of the basic approaches to civil security, and we completed our task in this unit by discussing various elements of risk education. I hope you have found this lesson very interesting and thought-provoking too. In the following unit, we shall be discussing three other approaches to civil security. Please, never hesitate to consult your tutorial facilitator, if any aspect of this study is not clear to you or reach your course coordinator to link you up with the writer of this instructional material if it is very necessary. Good luck.

6.0 TUTORED MARKED ASSINGMENT

a) What do you understand by the term civil security?
b) Write a short note on the meaning of risk education, and any three of its elements.

7.0 REFERENCES AND FURTHER READING

Dory, A.J. (2003a). *Civil Security: Americans and the Challenges of Homeland Security*. Washington DC: Center for Strategic and International Studies (September).

Dory, A.J (2003b). American Security: the US Public and Homeland Security. *The Washington Quarterly*, 27(1): 37-52.

Holton, G.A. (2004). Defining Risk. *Financial Analysts Journal*. 60 (6): 19-25.

Kennedy, J.F. (1961). Radio and Television Report to the American People on the Berlin Crisis. Washington, D.C. (July 25). Also available on .cs.umb.edu/jfk library/jfk_berlin_crisis_speech.html. Retrieved on 2 October, 2003.

Luhmann, N. (1996). *Modern Society Shocked by its Risks*. University of Hong-kong: Department of Sociology (Occasional Papers 17).

Shalamanov, V., Hadjitodorov, S., Tagarev, T., Avramov, S., Stoyanov, V., Geneshky, P., & Pavlov, N. (2005). In: *Civil Security: Architectural Approach in Emergency Management Transformation*. Sofia: ProCon Ltd/ *Information & Security: An International Journal*, 17: 75-101.

Weyman, A. & Shearn, P. (2004). *Teaching Practice in Risk Education for 5-16 Years olds*. Sheffield: Health and Safety Laboratory: Report Number HSL/2005/23.

Error! Hyperlink reference not valid.. Retrieved on 19 August 2009.

://portalnano.ru/files/20. Retrieved on 10 August 2009.

://www.bmbf.de/en/6293.php. Retrieved on 19 August 2009.

://www.unisdr.org/eng/public_aware/world_camp/2004/booklet-eng /Pagina 9ing .pdf. Retrieved on 19 August 2009.

UNIT 5

CIVIL SECURITY: MEANING AND APPROACHES II

CONTENTS

1.0 INTRODUCTION

In the last unit, we began our task on the meaning and aspects of civil security. The rationale behind invocation of the concept of civil security underscores the need to have the public playing complementary roles not only in security planning but also in the management of security. In as much as the public forms the nucleus of the stakeholding in the business of security, they should be involved in security activities so that they can care for themselves in the event of security attack. In this unit, we shall complete our task on the subject- civil security and its aspects. We have previously treated the meaning and one of the aspects (risk education) of civil security. Now, we shall be discussing the remaining three aspects not earlier discussed.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Explain other three aspects of civil security not treated in the last unit;

Discuss the meaning and elements of preparedness;

Examine the meaning and elements of public warnings; and

Describe protective actions and its elements.

3.0 MAIN BODY

3.1 **Preparedness**

Preparedness is another key element or component of civil security. Sometimes, one may be sceptical to support the view that states that for any community to prevent violence (war), it is incumbent on it to always prepare for violence (war). Here, the term violence or war is used to denote any (potential) threats or attacks from enemies such as armed robbers, kidnappers, saboteurs, terrorists, election riggers, computer hackers, assassins, militants, fraudsters, fire outbreak and accidents, among others.

It is always important to prepare oneself against the unexpected because it will enhance one’s capacity to prevent such security threat from occuring, and in the situation of its occurrence, the rate of damage will be minimal. For instance, Nigeria’s Federal Road Safety Corps usually campaigns for compulsory use of seat belt in order to reduce the fatality of accidents on our roads.

Again, some new automobiles now come with air bags to provide safety for the occupants of the vehicle in a situation of serious accident but the vehicles equipped with air bags still have seat belts because the manufacturers feel that the air bag system may fail to activate, and the seat belts can therefore provide a security back-up for the occupants of the vehicle when a serious accident occurs. The foregoing scenario demonstrates how important it is, to always prepare oneself against any hazardous situation. Now, what is preparedness? According to Amanda Dory, preparedness can be described as:

.....a method by which awareness and understanding (supported by risk education) can be translated into action........, and it can include a range of activities: developing contingency plans (e.g. communications, evacuation, shelter-in-place0, practicing contingency plans, participating in education and awareness activities, and stockpiling emergency supplies (Dory, 2003: 35).

Preparedness can also be described as:

.......a comprehensive plan (that) provides a range of scenarios with clearly defined, detailed processes and responsibilities. A critical component of a business continuity plan is a secure access plan to ensure remote or isolated emergency workers can continue working during and after a disaster (://www.juniper.net/us/en/solutions/public-sector/state-local-government/emergency-preparedness).

Conducting a surgical analysis on the foregoing definition, you may agree with me that preparedness is very fundamental to safety and security management. We cannot but agree with Boys Scout in their motto, which says ‘always be prepared’. Thus, preparedness enables the public to take active roles in risk management and effective participation in the process of security management. Preparedness helps security agencies and the public, if not to absolutely prevent attacks but at least to reduce the fear and anxiety associated with security threats. It can assist in reducing the fatality rate in the consequences of any security threat in physical, psychological and economic terms (see Dory, 2003: 35).

In addition, preparedness enables individuals to respond creatively to any situation of security attack, even without seeking for external intervention. Here, prepared individuals engage in activities to protect themselves and react very effectively to security threats by taking good control of the situation. This will limit the burden of security intervention by relevant government agencies. For instance, in some communities, people watch the activities of one another very closely and whenever any member is suspected to constituting a security threat to the whole people, the people act swiftly by asking the fellow to vacate the place or be handed-over to the police.

In the situation of attack of armed robbery, the people jointly put-up a strong resistance against the attackers whether or not the intention of the attackers aim a particular target. One of the ways to achieve this, is to adorn the community with street lights, and where or when there is no electricity supply from the energy agency (PHCN), some of the people can volunteer to use their generating sets to power those street lights unilaterally or on rotational basis.

Also, when the presence of strangers is noticed, people need to humbly accost them to know their mission. But caution should be exercised in doing this, they should make sure the strangers are not equipped with dangerous weapons before approaching them. In a situation where they are not sure, they should alert the Police promptly. In furtherance of our understanding of this subject, let us discuss various elements of preparedness. Before we do that let us have a five minute break. Break over!

Elements of Preparedness

a) Adoption of 'dual use' approach: The state and local governments due to nearness or proximity to the people should endeavour to build the capacity of the security sector and public not only in the areas that concern man-made attacks (i.e. terrorism, armed robbery, computer virus attack, computing system hacking, sabotage, corruption, spills, accidents etc) but also those that relate to threats that are natural such as hurricane, flooding, tornadoes, drought, earthquake among others.

It is very unfortunate that in Nigeria, the security sector let alone the civil public is not adequately trained to respond promptly and effectively to the incidence of terrorism within and without. One of the factors to this strategic deficiency can be traced to the lackadaisical and inept nature of various intelligence agencies. The moribund nature of our security infrastructure is another factor. Most countries in Europe have closed circuit Televisions (CCTVs) and surveillance cameras installed in every nook and cranny of their homelands not only to detect (perpetrators of) crime but also to prevent and/or reduce criminal activities. Even, if CCTVs are to be installed everywhere in Nigeria, the regular power outages will render these security materials less functional.

On reacting to natural disasters, the public can be said to have no adequate knowledge on how to manage the situation when natural disaster occurs. Even, experience has shown that the Emergency Management agencies in the country both at federal and state levels have appeared to be very incompetent and impotent in disaster management. For instance the way the Ikeja Bomb blast episode was handled rubbished the efficacy or simply the preparedness of the security sector in Nigeria and Emergency Management Authorities in disaster management.

This incident occurred on January 27, 2002 in Lagos where "several bombs exploded at the Ikeja Military Cantonment during which scores of thousands of people died during the stampede that followed the explosion particularly children that drowned in a chemically contaminated canal called Oke-Afa Canal in Isolo, Ejigbo Local Government Area (LGA)"(**Error! Hyperlink reference not valid.**). Ridiculously, it took the intervention of foreign bomb experts to detonate other bombs scattered all over the neighbourhoods;

b) Development of emergency preparedness materials: The government in collaboration with public and private sector(s) should establish local offices throughout the nation where people can easily access emergency materials like swimming jackets in case of flood, vaccines and medicals in situations like disease outbreaks or epidemics, among others;

c) Development and maintenance of sophisticated emergency response procedures, training and working tools for emergency workers. For instance, in ensuring quick response of the Police to any distress call, the communication systems and vehicles must be in good order. Also, it is paramount to provide security personnel with bullet-proof vests and other equipment that will make their job an easy one.

Thus, compared to police personnel in developed countries, men and officers of Nigeria Police are poorly equipped. This is instrumental to their poor state of their preparedness activities. It is most disturbing the way police stations are being attacked in recent times. This situation shows lack of preparedness by the police against any attack. If the police fails to protect itself, then, how can it protect the public? This leads to the following point or condition;

d) Regular conduct of simulation: Simulation is very essential to preparedness. It assists to present to the security personnel, the true reflection or state of their preparedness to various security threats. There is no doubt that regular conduct of simulation will enhance the capacity of security personnel to identify their areas of vulnerability, through which they can fathom ways to address it and improve their preparedness; and

e) Educating the Public: Educating the public on security issues is a key element to risk education, which will increase their awareness of possible security threats, so that they can prepare themselves against the occurrence of security attacks. And when a security attack happens, they can easily be on top of the situation by refusing to be overwhelmed by fear and anxiety. For example, had it been there had been public enlightenment on security threats and disaster management, the casualty rate resulting from the Ikeja Cantonment bomb blast episode, would have been minimal. The fact is that people would have had enough awareness to avoid panic in situations like that. Therefore, many of the victims would not have jumped into the Canal out of confusion.

SELF ASSESSMENT EXERCISE

How do you define preparedness?

Explain the elements of preparedness.

3.2 Public Warning

The importance of prompt and effective public warnings in responding to natural and/or man-made disasters or security threats cannot be over-emphasized. The truth of the matter is that public warnings assist the public to take actions that can save lives, reduce fatality and enhance their recovery capacity. According to the Partnership for Public Warning in its report titled "Developing a Unified All-Hazard Public Warning System", , warning can be described as a 'process' that:

.....consists of people with information communicating with people at risk, and others such as emergency responders, in advance of or during a hazardous event, with the intent that those at risk will take appropriate action to reduce casualties and losses. The goal of warning is to prevent hazards from becoming disasters. The success of a warning is measured by what actions people take (Partnership for Public Warning (2002: 3).

Warning can also be described as:

a communication and acknowledgment of dangers implicit in a wide spectrum of activities by potential opponents ranging from routine defense measures to substantial increases in readiness and force preparedness and to acts of terrorism or political, economic, or military provocation (Dictionary of Military and Associated Terms 2005.).

....something that serves to warn, give notice, or caution (**Error! Hyperlink reference not valid.**).

.....admonition, notice, or pointing out an existing or potential danger, specially to one who would otherwise would not be aware of it (**Error! Hyperlink reference not valid.**).

Public warnings involve activities designed to alert the public on the impending danger. The foreign ministries of several countries take it as a matter of priority to alert their citizens of the inherent danger of travelling to some countries through the media and internet. Even, if some of the citizens will still wish to travel to those countries considered as unsafe, the alert will assist them to prepare themselves, and plot ways to mitigate the effect of fear and anxiety and building their capacity to responding to security attacks or threats. This can at least help them reduce losses in the event of experiencing attack.

During a hazardous event, people can be notified with the aim of alleviating or forestalling further losses. This is done to enable people to proffer actions to mitigate the risk that underlies a security threat. For instance, in a situation of fire-outbreak in a business building, the people in the building are to be notified of the incident, and they should be advised not to panic. Thereafter, they should be guided on how to exit the building. The basis of public warnings is to prevent hazards from leading to disasters. Disasters involve huge loss of lives and property, which should be avoided as much as possible. What determine the success of any warning initiative are promptness of the intervention and appropriate actions. If any public warning lacks any of these two elements, it will be difficult for such warning to attain the desired goals.

Elements of Public Warning

a) Data collection, analysis, and decision-making to issue a warning: Evidence of a hazard must be developed through data collection, and the collected data analysed. After the analysis, we can thereafter make a decision in issuing a warning. The procedure is very necessary to observe in order to avoid raising an unnecessary and false alarm that may affect the people’ response to future warnings. For instance, if the farmers in a particular settlement are warned of the impending drought in a particular year, many of these farmers may relocate to another area for cultivation or not to engage in farming activities at all during that period.

   And if it is found at the end of the day that the situation of drought never occurs against the earlier public warning, it will be difficult to convince the affected people of an impending security threat in future warnings. In a situation like this, people will disregard the warnings until they begin to experience the hazards, and if no appropriate measures of intervention are taken, such hazards like earthquake may lead to disasters resulting in huge loss of lives and property, where the effect of the hazards could have been minimized if there had been adequate preparedness by the victims in the first instance (see Mileti & Sorensen, 1990).

b) Framing a warning: it is also important to identify the right words and digitally coded warning message that involve the application of standards for terminology also putting into consideration the most effective ways to communicate warnings to the target audience. If a warning is meant to be communicated to civilians, it is appropriate to avoid using codes but rather to communicate in the language format that they will understand.

   This may be difficult in a multi-lingual society like Nigeria where there are several ethnic groups with different languages. It is more problematic because it is not everybody that understands the official language (English), and it is necessary to translate the warnings into the local languages of the target population. And where some the people can neither understand English nor any of the translated languages, it will be up to the people who understand to pass the information to the affected people;

c) Use of Secure Sources: Getting inputs from dependable and authorised sources is very germane to public warning apparatus. These authorised sources help not only in the collection of objects of warning but also assist in delivering warning to various targets;

d) Transmission of warnings: Transmission of warnings should be handled very professionally, and it demands the use of a wide variety of distribution systems such as telephone, internet and public address system, to mention a few. The arrival of GSM in Nigeria has been helpful in providing warnings to the public in case of any security threat or hazard. For instance, if an incident of bank robbery is taking place in a particular location, one can easily be alerted through a voice call or short messages (SMS) of the risk of being in that location at that particular time because of the possibility of being hit by bullet. Meanwhile, one great obstacle to the use of most of the warning facilities is the erratic nature of power supply in Nigeria; and

e) Human Attitude to warnings: it is one thing to issue warnings to people against a security threat or hazard but it is another for the people to whom the warnings are made, to respond appropriately and timely to the warnings. Undoubtedly, warning has no relevance or importance if people fail to ‘hear and respond’ (Dory, 2003: 55). For instance, in many urban centres in Nigeria, people often turn deaf ears to government warnings to vacate buildings considered to be a threat to the security of the occupants because of the risk involved in staying there. The reason may be due to high cost of securing another accommodation. Therefore, it is important on the part of government to provide cheaper accommodation for the people through development of low cost housing scheme as well as drastic reduction in the cost of building materials.

SELF ASSESSMENT EXERCISE

Briefly describe public warning and its elements.

2.3 Protective Actions

Protective actions are the most critical component as well as the climax of the civil security agenda. It involves the steps which the public can take to alleviate or reduce the adverse effects that any natural or/and man-made security threats or hazards can have on them. This component of civil security comes after exploring three other elements of civil security including risk education and communication, preparedness and public warning. In order to have a greater knowledge of the subject matter, it is pertinent at this juncture to explain its fundamental elements.

Elements of Protective Actions

a) Evacuation: This is usually a popular practice in protective action. Apart from natural and man-made threats that are premeditated such as assassination, arson among others, there are other man-made threats that are accidental. Accidents occur almost on daily basis. On the roads, accidents do occur may be through carelessness or recklessness as the case may be or human error. For instance, some people are in the habit of over-speeding when driving despite the regular campaign by the Federal Road Safety Corps (FRSC), calling on road users to avoid reckless driving and over-speeding. In industries, accidents do occur ranging from fire-outbreak, suffocation, spilling of harmful chemicals, to mention a few. Many industrial workers have had their hands amputated by machines resulting from human error or fatigue.

The industrial inferno episode that occurred in a factory located at Ikorodu, Lagos state still linger in the memory of many Nigerians especially the families, friends and close relations of the victims of the fire-outbreak which claimed the lives of the workers working in the factory. The death toll would have been reduced if there was prompt or timely evacuation response, and it was most pathetic that the victims were unable to escape because the management allegedly locked them up in the factory, meaning there was no exit point for safety.

Sadly, that phenomenon speaks volumes of the state of enslavement that most Nigerian employees are subjected to by their ‘masters’. In order to forestall the repeat of such an incident, it is important for the government to criminalise all dehumanising policies of employers or managements against their staff or employees, and adequate punishment should be meted on the erring employers including life imprisonment.

Again, the issue of terrorism should be given priority attention by Nigerian government. If the incidence of terrorism is less evident or not existing at all in the country now does not depict that Nigeria is immune to terrorist attacks considering the presence of anarchist ethno-religious groups in the country. No one could believe that Kenya and Tanzania could become targets of attack by terrorists until it happened. The terrorists planted bombs at the US embassies in those two countries, which later exploded killing and injuring hundreds of people, most of whom were Africans. Resulting from those bombing incidents, one cannot say that since Nigeria is not a party to the Middle-ease crisis, it cannot be a target of Arab insurgents. Therefore, it is very important for the security sector to develop a framework through which they can respond promptly and adequately with appropriate evacuation actions in the event of a terrorist attack;

b) Sheltering or Shelter-in-Place: This element of protective action can be described as “practice of remaining indoors in an office, home, school or other structure; or if outside, taking refuge in a nearby building in order to minimize the effect of a hazard” (Dory, 2003: 68). Sheltering is a crucial protective action that involves a variety of withdrawal actions.

It is easier to facilitate sheltering than evacuation because it does not take much time to undertake, as few studies have shown that individuals would need “five to ten minutes to take shelter after they receive the alert or notification to do so” (Dory, 2003: 69). But, if the findings of Rogers et al. are anything to go by, any expedient sheltering actions like sealing of windows, doors as well as other opening should take between three and thirty-nine minutes but seventeen minutes on the average to undertake (Rogers *et al.* cited in Dory, 2003: 70);

c) Quarantine and Shielding: Let us begin our conceptual illumination of the two terms by defining quarantine. Quarantine can be simply defined as officially imposed isolation or a way of separating an infected person from the rest of the people with the aim of curbing the possibility of the spread of the disease due to the efficacy of such ailment to pose a great security threat to public health. For instance, it is incumbent on the government to quarantine a member of the community infected with laser fever because of the virulent and infectious nature of the disease;

d) Medical Counter Measures (MCM): These are also crucial elements of protective actions. They usually involve a wide spectrum of medical interventions and treatments that can be applied in the event of a hazard or security attack. This element of protective actions is so vital because it provides an opportunity to counter or mitigate the adverse effect that any security attack may have on the people especially through availability of drugs and medical treatment. For instance, in some homes in Nigeria, families have first-aid equipment because they are aware that accident can happen anytime at home, so that they can give first-aid treatment to person in medical need before taking him/her to the hospital for further treatment. This can help to reduce the damage from any incident of security threat or hazard.

   As a matter of protective engagement, government is expected to develop Strategic National Stockpiles (SNS) for medical countermeasures. The SNS should be stocked with vaccines, antivirals, anti-toxins, anti-snake venom (particularly there is regular incidence of snake bites, notable in northern Nigeria), anti-malaria drugs, among others. SNS should have centres in all the local governments in the country for easy access by the public especially in the event of epidemics like cholera, small-pox and polio; and

e) Individual Protective Equipment: As discussed above, some individuals appreciate the need to pay priority attention to issue concerning their safety and security. For instance, in Nigeria, many people have died when the boats they were travelling with capsized in the middle of the river or sea. Meanwhile, many of the victim-passengers would have survived, if they had life-saving jackets, which could still make them float on water till rescue would come to them. Nevertheless, security and personal safety demands that it is important to purchase necessary protective equipment for private use. It is very funny that most of the road users in Nigeria drive their vehicles without having fire-extinguisher. Some do not even have extra tyre(s).

SELF ASSESSMENT EXERCISE

Define protective actions, and write short note on any four of its elements.

4.0 CONCLUSION

In as much as it is popularly believed that the end product of every security activity is supposed to be towards meeting the security needs of the people, it is pertinent to engage the public in active roles in the security of their communities, not by carrying out jungle justice against any crime suspect(s) but by providing useful assistance to the law enforcement agents and emergency workers. More importantly, through active participation, people should learn ways to take care of themselves in order to reduce losses in the occurrence of hazards or security attacks. People who are familiar with all the aspects of civil security will always have capacity to handle any emergency or hazards more creatively and effectively too, than persons who lack knowledge of civil security activities. The good news is that there has been increasing participation of the public in security decision-making process, as security is not more seen as the exclusive function of the government. People now take more active roles in security planning and management, and the springing-up of private security players is very evident as well.

5.0 SUMMARY

In this unit, we studied various other approaches to civil security that we were unable to treat in the last unit. We began our task by describing preparedness as an approach to civil security. Thereafter, we examined the meaning of two other approaches including public warning and protective actions as well as their different elements.

6.0 TUTORED MARKED ASSIGNMENT

Write short notes on any of the following:

1) Preparedness and any four of its elements
2) Public warning and any four of its elements.
3) Protective actions and any four of its components.

7.0 REFERENCES AND FURTHER READING

Dictionary of Military and Associated Terms (2005). US Department of Defense.

Dory, A.J. (2003). *Civil Security: Americans and the Challenges of Homeland Security*. Washington DC: Center for Strategic and International Studies (September).

Mileti, D. & Sorensen, J. (1990). *Communication of Emergency Public Warnings*. Oak Ridge National Laboratory (ORNL).

Partnership for Public Warning (2002). *Developing a Unified All-Hazard Public Warning System*.

://allafrica.com/stories/200801280937.html. Retrieved on 18 August, 2009.

://dictionary.reference.com/browse/warning. Retrieved on 20 August 2009.

://www.businessdictionary.com/definition/warning.html. Retrieved on 20 August 2009.

://www.juniper.net/us/en/solutions/public-sector/state-local-government /emergency-preparedness. Retrieved on 19 August 2009.

MODULE 4

UNIT 1

MEANING OF INTELLIGENCE

CONTENTS

1.0 INTRODUCTION

The experience of the world since World War II has shown that security management is a very serious business. It is not surprising that the security sectors both nationally and internationally have undergone a number of reforms aimed at addressing security challenges and threats that bedevil the world population. There is no doubt that one of main areas of attention in security is intelligence. Intelligence has become one of the key elements of security sector reform. This explains why state and non – state actors currently invest huge amount of resources both in human and material terms on intelligence. It is against this background that we find it important or germane to use a number of units in this course to conceptualize intelligence and to look at its practical application, dimensions, categories, collection, analysis, evaluation among others. In this unit, we shall be focussing on the definition of intelligence and some of its uses. Let's quickly take a look at the objectives of this unit.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Define the term intelligence;

Discuss the dimensions of intelligence;

Explain the categories, of intelligence; and

List the source of intelligence.

3.0 MAIN BODY

3.1 Defining Intelligence

The term intelligence is often mistaken for information or data. This is because most people (or simply the laymen) usually describe it to mean information. However, intelligence is different from (ordinary) information although it is a form of information, which has been ingrained with added value through analytical and evaluative instrumentation. Intelligence is a refined, analysed and evaluated information or data gathered through either overt (open) or clandestine (secret) means or both.

The conceptual differentiation between information and intelligence can be described "….. along a continuum, with data at the far left and intelligence at the far right, as one moves from left to right additional value and context is added to discrete or posited facts to provide enhanced meaning to an ultimate consumer" (**Error! Hyperlink reference not valid.**). As discussed in the introductory segment of this unit, intelligence has attracted growing interest among scholars and security corporations. Thus, various intellectual efforts and articulations by these groups of people have yielded fruits in academic discourse and one of such is conceptualization of the term (intelligence). Therefore, several definitions have emerged among which include the following:

Intelligence...is not only about spies and satellites. Intelligence is about the thousands and thousands of routing everyday observations and activities. Surveillance, interactions – each of which may be taken in isolation as not a particular meaningful piece of information, but when fused together, gives us a sense of the pattern and the flow....(.Fas.org/sgp/crs/Intell/RL 33616.pdf).

Intelligence ……… is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspect of foreign nations or areas of operation which immediately or potentially significant for planning (the Dictionary of United States Military Terms Joint Usage).

Intelligence is a special kind of knowledge, a specialized subset of information that has been put through a systematic analytical process in order to support a state's decision and policy makers. It exists because some states or actors seek to hide information from other states or actors who in turn seek to discover hidden information by secret or covert means (Hannah et al, 2005, iii).

Intelligence can also be described as what a "state must possess regarding other states in order to assure itself that its cause will not suffer nor its undertakings fail because its statemen and solders plan and act in ignorance" (Kent, 1966:3). It usually involves the gathering, sorting and ranking various data collated according their respective degree of importance to relevant security issues or problems under scrutiny and (scientifically) analysing those information to identify ones that can assist us or policy makers in decision-making process. Intelligence In recent times, intelligence has not only become a key element of security management but also the heartbeat of security in modern time. This is because its impact on security cannot be under-estimated. In the next segment of this unit we shall be looking at the various dimension of intelligence.

SELF ASSESSMENT EXERCISE

How do you define intelligence?

3.2 Dimensions of Intelligence

As preceding discussions will have demonstrated, intelligence, conceptually, interpretes itself in various forms, according to how each individual or state perceives it. The British intelligence officials are used to saying that "intelligence is about secrets, not mysteries" (see Davies, 2002). By and large, intelligence involves analyzing and evaluating information collected through open and secret means. In intelligence community, interpretation of gathered information for intelligence purposes usually exhibit itself in three dimensions which include:

a) Intelligence as a process: Here, intelligence is described as a process through which information is collected or gathered. After information has been collected and collated, such information will then be subjected to systematic analysis and evaluation. Intelligence process is very important, as it allows us after collecting the raw data, to separate the information that are useful from those that are not useful.

   During this process, values are added to information which make it (information) refined "into a usable form for decision makers" (Hannah *et al.*, 2005: IV). There is no doubt that, it is often said that "the relationship between processes and structure … determines the successful outcome of the intelligence activity" (Ibid);

b) Intelligence a structure: This is all about the agency or agencies and institution(s) charged with the responsibility of intelligence sourcing for consumer i.e. the government. The institutions (often referred to as intelligence services), in carrying out their intelligence activities, they are influenced by a number of factors. According to Hannah et al, 2005: iv), these factors may include:

   i. The roles and mandates adopted by one or more services (i.e. are there different agencies for both the domestic and foreign role?) – as well as understanding overlaps between intelligence agencies and other players (such as law enforcement) in the security community;

   ii. The shape of any central analysis and / or assessments mechanism to process collected intelligence;

iii. The need to ensure central control and coordination of and accountability for, the intelligence community; and

iv. The need to ensure pubic oversight of the intelligence community.

There are several overlapping aspects, or rather types of intelligence such as security intelligence, domestic intelligence, military intelligence, to mention a few, which according to each nation, maybe separated by delegating different agencies with different categories of intelligence. In this case, each intelligence agency will be tasked with a category of intelligence. In Nigeria, the intelligence unit of the Nigeria Police is mandated by the law to carryout home–security intelligence while the Directorate of Military Intelligence (DMI) performs the task of providing military and strategic intelligence.

By and large, countries decide on the (possible) framework to adopt in intelligence activity. Some countries divide various intelligence roles to be played by different intelligence services that operate independent of one another but within the approach of complementing functionality. In other words, despite being independent of one another, the intelligence services or institutions must act to complement one another's roles for system maintenance.

On the other hand, there are countries where there exists only one intelligence agency, which performs all intelligence activities ranging from domestic to foreign, at the same time. A good example was KGB in the defunct Soviet Union. A caution has to be exercised here, and this is because having one intelligence service or agency performing all intelligence functions does not always mean that there exists only one intelligence service. The number of available intelligence services varies from country to country.

Sometimes, there may be plurality of intelligence agencies in a state, and among them, there may be a single agency that can perform all intelligence activities. For instance, in the United States, in practical terms, there are several intelligence outfits or agencies that perform various intelligence functions but the Central Intelligence Agency (CIA) performs all functions ranging from domestic, paramilitary to foreign intelligence.

However, the art of separating various forms of intelligence functions (domestic, military foreign etc) demands that there should be proper coordination of such tasks among various agencies particularly as it concerns the cross border security threats such Cyber war, terrorism and others. In some cases, intelligence services, though separate from one another, may be mandated to perform all intelligence activities and functions. Thus there will be a body that will coordinate, collate and synthesize various intelligence reports coming from all the intelligence services through (scientific) analysis and evaluation of the information collected. On the question of accountability, in some countries, the intelligence services are answerable to the legislature while in some political systems like Nigeria, the executive controls the intelligence service;

c) Intelligence as a product: The intelligence services undergo the process of collecting information, which will be analysed and evaluated. After analysis and evaluation, the information gathered will become refined, and ready to be used by the consumer to meet its short and long-term goals. It is worth-nothing that, in contemporary time, intelligence consumers are not only governments. This is because corporate individuals and organizations can also seek for the services of intelligence agencies in the provision of some specific intelligence, which may be strategic to their decision–making and security.

   As discussed, the outcome of any intelligence activity is determined by the relationship between the process and structure. Here, the outcome is the product of the intelligence. According Hannah (2005) intelligence–product is aimed at assisting the consumer(s) to address ‘foreign or external threats’, threats to national security’, as well as providing ‘advice on policy and decision–making’.

SELF ASSESMENT EXERCISE

Discuss the dimensions of intelligence

3.3 **Categories of Intelligence**

There are several categories of intelligence and these include the following:

a) Security Intelligence: This form of intelligence, according to Kent (1965:209-210) can be described as:

   ...the intelligence behind the police function...the knowledge and the activity which...defensive police forces must have before they take specific action against the individual ill-wisher or ill doer.

   Security intelligence usually involves collecting, collating, analyzing, evaluating and disseminating information that can protect a nation against internal threats;

b) Criminal Intelligence: This is a kind of intelligence activity or function carried out by the relevant service or intelligence agency to provide evidence in support of prosecution of any criminal suspects. Take for instance, before a suspect can be arranged in court by the police, it is expected that enough information must have collected, analysed and evaluated, which will help the court (as the consumer) to make a decision on the suspects.

Infact, it can be argued that lack of adequate criminal intelligence has been a great challenge to the prosecution of criminal (suspects) in Nigeria. It is really disappointing that Nigeria police and State Security Service (SSS) have failed to bring any of the perpetrators of political assassination which the country has recorded in the last eight years to book (see Onyeozili, 2005). Several suspects have been prosecuted in court(s) but nobody has been indicted, since there is no sufficient criminal intelligence to indict nail the accused;

c) Home security or National Intelligence: It is that intelligence, which involves gathering, collating, analyzing and evaluating as well as disseminating information within a given state for the effective management of national security. The national intelligence is reinforced by integrating intelligence within wide spectrum of nation al strategy mechanisms that go beyond unilateral competences or needs of a single department' (Hannah, 2005:2);

d) Foreign Intelligence: This is a traditional form of intelligence in which the intelligence activity takes place outside the home country. The importance of this intelligence to the strategic intelligence of any nation cannot be over-emphasized. This explains why Ambassador John Negropontes, in his speech before the United States Chamber of Commerce (cacophonically) submitted that "what happens abroad can kill us at home".

Negropontes' submission is apt, considering the emergent 'villagelization' of the world system where globalization has broken the (traditional) barrier among nations not only in geographical terms, but also economically, politically and socially. The world has become a global village. Foreign intelligence allows a country to have strategic information about foreign nations' activities and how such activities constitute a threat to her security, as well as what counter – measures can be adopted to such external threats;

e) Strategic Intelligence: This category of intelligence tends to focus basically on gathering, analyzing and evaluating about the capabilities, vulnerabilities and aims of foreign countries. In doing this, the country will have an opportunity to identify its Strengths, Weakness, Opportunities and Threats (SWOT Analysis) in the time of peace and provides a platform. This will enable such a country to develop a framework for strategic military operations in case there is war in the nearest future.

It's on the basis of the strategic intelligence outcome that the policy and decision makers will on which programme(s) to adopt. Net assessment can be adequately conducted by any country or party. Such strategic intelligence that are developed will assist decision makers to take into account fundamental uncertainties about the future. Net assessment involves developing an analytical framework that takes into account the strategic goals, doctrines, operational concepts and strategic military capabilities of competing countries, alliances as well as several other international actors;

f) Tactical Intelligence: This involves devolution of responsibility among the hierarchy of personnel in an intelligence service such that information are collected, collated, analysed and evaluated for the use by the leadership or top management for short term policy agenda; and

g) Counter-intelligence: This involves measures to counter any foreign intelligence activities, capable of constituting a threat to national security (Ramsokn, 1958). It also includes launching intelligence operations to arrest or destroy the human intelligence capabilities of the enemy states (hostile countries).

SELF ASSESSMENT EXERCISE

Discuss any five categories of intelligence.

3.4 **Sources of Intelligence**

As already discussed, intelligence actually involves collecting and refining information with the aim of coming up with information that can be useful for investigation or decision-making process. In the course of preparing intelligence, a number of sources can be used in gathering information for the intelligence process, and what are these sources? There are several sources for intelligence collection, and they include the following:

i. Member(s) of the public;

ii. Foreign governments;

iii. Intelligence personnel;
iv. Communication technologies;

v. Open sources like newspapers, academic journals, unclassified government documents, treaties etc;

vi. Internet; and

vii. Government institutions, etc.

SELF ASSESSMENT EXERCISE

Highlight any five sources of intelligence

4.0 CONCLUSION

Intelligence has remained crucial in security management. Since the end of World War II, intelligence has assumed a new dimension, and it has formed the large part of strategic planning and securitization agenda of the world powers particularly it related to prevailing ideological polarism. Providing adequate (and effective) intelligence can assist an organisation (or country) with a wide range of opportunities, including assessing the risk and threats that can undermine the internal security of that organisation or country. Due to the strategic importance of intelligence, it is quite paramount for services to conduct regular intelligence reform to meet the challenges of modern security sector.

5.0 SUMMARY

In this unit, we focused on the meaning of intelligence. We began the study by defining the term intelligence. Also, we discussed the various dimensions of intelligence. In the segments, our attention was drawn on explaining categories of intelligence. The fourth subject of discourse was highlighting the sources of intelligence. I strongly believe that you've found this unit very interesting. But, if you have problem understanding any segment or whole of this unit, feel free to consult your tutorial facilitator who will assist in the areas of difficulty, if there are any.

6.0 TUTORED MARKED ASSIGNMENT

(i) What is Intelligence?
(ii) Discuss any four categories of intelligence.

7.0 REFERENCES AND FURTHER READING

Davies, Philip H. J. (2002), "Ideas of Intelligence: Divergent National Concepts and Institution", Intelligence, Vol. 24 (3), Fall. Also available on **Error! Hyperlink reference not valid.**. Retrieved on 8 April, 2008.

Hannah, G., O'Brien, K. & Rathmell, A. (2005). *Intelligence and Security Legislation for Security Sector Reform*. Cambridge, UK: RAND Europe.

Kent, S. (1965). *Strategic Intelligence*. Hamden, Connecticut: Archon, Books

Kent, S. (1966). *Strategic Intelligence for American World Polity*. New Jersey: Princeton University Press.

Lowenthal, M. (2000). *Intelligence from secrets to Policy*. Washington DC: CQ Press.

Michael C. (2006). Remarks at the Bureau of Justice Assistance and SEARCH symposium on "Justice and Public safety information sharing" on 14 March, 2006. Also available on .fas.org/spg/crs/intel/RL 33616.pdf. Retrieved on 12 March, 2008.

Onyeozili, E. C. (2005). Obstacles to Effective Policing in Nigeria. *African Journal of Criminology and Justice Studies* 1(1): 32-54.

Ramson, H. (1958). *Central Intelligence and Nations Security*. London: Oxford University Press.

.en.wikipedia.org/wiki/Intelligence. Retrieved on 6th March, 2008.

UNIT 2

INTELLIGENCE COLLECTION AND DISCIPLINES

CONTENTS

7.0 References / Further Reading

1.0 INTRODUCTION

Intelligence has several areas and one of them is information collection. Therefore, there is division of labour among intelligence officers according to their areas of competence in intelligence profession. The foundation of any intelligence work or production is found in the collection of raw data which the (intelligence) analysts will refine and turn out as intelligence product. In intelligence community (IC) efforts are made (in an attempt to produce intelligence) towards looking for data useful for intelligence production. The process of collecting information for intelligence purposes is known as intelligence collection. In thus unit, we shall be focusing on intelligence collection as well as a wide range of issues concerning intelligence collection.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Define intelligence collection;

Identify various disciplines of intelligence collection; and

Explain means of intelligence collection.

3.0 MAIN BODY

3.1 Defining Intelligence Collection

Information is very crucial to carrying out intelligence tasks. This means that the art of collection of information must first be considered, in intelligence business. We can at this point pose a question: what is intelligence collection? It can be defined as “the procurement of information believed to be pertinent to a decision-maker (sometime referred to as ‘raw’ intelligence data)” (Hannah et al, 2005:1). Intelligence collection can also be described as a process of gathering and assembling information through several methods for the purpose of producing intelligence.

3.2 Disciplines of Intelligence Collection

In the intelligence community, there are several intelligence-collection disciplines that assist professionals in the collection of intelligence aimed at providing support for policy makers in their choice of a particular policy direction or the other. Intelligence collection disciplines can be divided into two: technical and non-technical means. The technical forms of intelligence disciplines include Signals intelligence (SIGNIT), Imager of Intelligence (IMINT), and measurement and signatures intelligence (MASINT). On the other hand, non-technical intelligence disciplines include Human

Intelligence (HUMINT) and Open Source Intelligence (OSINT). Now let us explain them one after the other.

Technical Intelligence Collection Disciplines

Signals Intelligence (SIGNIT): This involves gathering intelligence through interception or seizing of electronic communications;

Imagery Intelligence (IMINT): This involves the use of satellite images for the collection of intelligence. It is a method of collecting information through the use of snapshots to provide security; and

Measurement and Signatures Intelligence (MASINT) is scientific and technical intelligence. Here, information is gathered through "quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same" (see .fas.org/irp/program/masint.htm). There are several forms of MASINT, and they include:

Radar Intelligence (RADINT);

Acoustic Intelligence (ACOUSTINT);

Nuclear Intelligence (NUCINT);

Radio Frequency/Electromagnetic Pulse Intelligence (RF/EMPINT);

Electro-optical Intelligence (ELECTRO-OPTINT);

Laser Intelligence (LASINT);

Materials Intelligence;

Unintentional Radiation Intelligence (RINT);

Chemical and Biological Intelligence (CBINT);

Directed Energy Weapons Intelligence (DEWINT);

Effluent/Debris Collection; and

Spectroscopic Intelligence (see .fas.org/irp/program/masint.htm).

Non Technical Intelligence Collection Disciplines

Human Intelligence (HUMINT): This involves covert or secret collection of intelligence through human sources. A good example is espionage; and

Open Source Intelligence (OSINT): It involves collection of intelligence through public sources like archival resources, government documents, academic and professional materials, media etc. This collection discipline gathers information through non-secret sources, and it also plays a crucial role in the production of intelligence.

Marl Lowenthal, in his work, Intelligence: from Secrets to policy, argued that "Despite the fact that OSINT has always been used, it remains undervalued by significant segments of the intelligence community".

SELF ASSESSMENT EXERCISE

Explain the disciplines of intelligence collection.

3.3 **Means of Intelligence Collection**

a) Espionage: This usually involves the art of covertly or secretly collecting information through the use of human sources. According to the United State Department of Defense (DoD), espionage refers to "the act of obtaining, delivering, transmitting, commenting or receiving information about the nation defense with an intent, or reason to believe, that the information may be used to the injury of the United State or to the advantage of any foreign nations" (US Dept of Defense, 2007).

Spying or espionage is a traditional intelligence system in which some individuals are appointed on full time or part time basis, to work for some government(s) or intelligence agencies (either private or public) to steal valuable or important information from enemy targets with the aim of having strategic advantage over them. The set of people used for espionage include:

Agent: Agents are also known as assets. They are spies who gather information. They are involved in all sorts of clandestine reporting, sipping (or stealing), and illegitimately breaking into the information (systems) of their target parties, i.e. nations, business organizations, security agencies among others;

Case Officers: The business of spying is structured in a cell form. Spies are grouped in small units, and spies can only know other spies in their cell(s) or unit(s). It is the case officer who recruits his/her own spies. He/she must demonstrate some level of competence, understanding and professional maturity. He/she must also be a good team coach, having mentoring potentials to be a role model to the spies or agents working under him/her and

Courier: Couriers are support personnel who assist the spies in managing their clandestine communication by securing them (the communications) against enemy's interceptions or detection;

b) Black bag operations: These are clandestine or secret) ways of making (illegitimate) entry into the information facility(ies) of any target party for intelligence purpose(s). The methods may include lockpicking, safecracking, finger-printing, electronic surveillance, mail manipulation, forgery among others;

c) Interrogation: This involves putting questions to person(s) with the aim of getting information which can aid intelligence collection. There are various ways through which person(s) can be interrogated. These methods of interrogation include:

Suggestibility: This a kind of interrogation technique in which people or person being interrogated are (is) subjected to sleep deprivation or exposed to continual white sound etc.

Reid: This technique involve interrogators watching the body language of the person(s) (or suspects) being interrogated. This method is questionable because it is (very) difficulty to read the mind of man through his/her face or so-called body language;

Deception: Here, the interrogator applies deceptive mechanism or lie to confuse and make the suspect to vomit information that may assist in producing criminal intelligence. The investigator may lie to the suspect that he/she had been implicated by some other person(s) and there is need for him/her (suspect) to assist, sometimes, the interrogator promises the person being interrogated some incentive, just to deceive the suspect in order to get information from him/her; and

Torture: This is a process of interrogating a person (suspect) and getting information from him/her through infliction of extreme physical pain. Law enforcement agencies often apply torture technique on suspects to make confessions. Torture includes severe beating jaw breaking, head breaking, face and/or body mutilation, rib-crushing among others. This technique is obsolete and not effective because of the tendency of the person being tortured to make false confessions (or give false information) due to the extreme physical pain he/she suffers. Even if one is innocent or does not have (the needed) information, in the face of torture, the person may resolve to give false information as to escape further torture.

d) Number Stations: These are (covert) short wave radio stations. The voices that are heard on these stations are often created mechanically in various languages. The voices on the radio can be generated to represent or look like those of women or men as well as adult or children. Number stations are used in passing instructions or messages to spies or used to deceive the public or the government (management) of the target countries (organizations);

e) A One-Way Voice Link (OWVL): This is another form of shortwave radio in which transmission is targeted towards aiding communication flow between the spies or agents (working on the field) and their respective intelligence agencies (employers). This system allows the spies to transmit already recorded message without having to stay on air for so long;

f) Steganography: The term steganography emanated from the Greek, meaning "covered or hidden". This technique involves sending information to the recipient in a hidden way. The messages are concealed in such a way that they are hardly noticed. Examples of steganography include invisible ink, chaffing and winnowing etc;

g) Cryptography: This is the art and process of writing in secret characters. This technique is different from steganography because the message is not hidden but it is the meaning of the message that is coded while steganography primarily deals with how we can write hidden messages;

h) Concealment Devices: These are devices that we can secretly hide information or things (i.e paper) and they will look like ordinary object. Examples of these devices may include (special) books (especially religious materials), candles, coin etc;

i) Diversion Safe: This is a device which can be left open while concealing some information materials in its hidden compartment that can be hardly noticed by anybody;

j) Eavesdropping: This is a method which involves one secretly listening to a private conversation or discussion. People often do this by pretending as if they're deeply asleep but listening to conversation between some other parties. Eavesdropping occurs everywhere. Some people may deceive other people as if they have left but only to hide in a corner with the aim of listening to the conversions of other people secretly;

k) Surveillance: This is the act of watching people or objects. In contemporary time, the art of surveillance has gone beyond observing or watching (closely) the movement or behavior of people through human monitoring. It also includes monitoring through electronic gadgets and (other) technological and non-technological methods. Technological methods include telephone tapping, closed-circuit television, reconnaissance aircraft, internet and computer surveillance, GPS tracking, binoculars, postal interception, bugs (covert listening devices), etc. There are several other types of surveillance and these include:

Biometric Surveillance: It is the use of technologies to measure and study the physical and behavioral features of person(s) for the purpose of authentication, identification or screening. The physical features that (some of) these technologies analyze include eye retinas and irises, DNA fingerprints etc. The behavioral features may include signature, voice, gait etc. It is important to note that biometric surveillance is still a subject of further research; and

Natural Surveillance: Such models like crime Prevention through Environmental Design (CPTEI) and Defensible Space. This technique underscores the importance the character of society has in influencing the behavior of anybody attempting to commit crime. It is popularly believed that people are often skeptical of going into crime, if there is high risk, and 'natural surveillance occurs by designing the placement of physical features, activities and people in such a way as to maximize visibility and foster positive social interaction'
(see .en.wikipedia.org/wiki/Natural_surbveillance);

l) Pseudo Operations: These operations are often targeted towards collecting strategic information for intelligence purposes. They are usually adopted by states (nations) to locate and break into the insurgent areas by sponsoring a number of state agents who will pretend to be sympathetic to the cause of the insurgents. These state agents (defector) deceive the insurgents by fighting along with them, the government forces (Cline, 2005).

Basically, the aims of carrying out pseudo operations may include collection of vital information for long term or short term intelligence, or covert activities like assassination of palpable foes or decimation of the enemy's ranks etc. Law enforcement agencies particularly the police usually apply this technique by sponsoring defectors to enemy's camp to pose as if they are also anti-government;

m) Political Campaigning: This is another means through which intelligence can be collected. In several societies like Nigeria, a number of people who are supporting a candidate may decide to pose as some of the admirers of the opponent candidate with the intention of getting information that can nail or deny the opponent of the anticipated victory. All the decision secretly arrived at in the opponent's camp are revealed to their camp. The people who're used to carry out such intelligence task can be regarded to as "Straw men".

I could remember in 2003 gubernatorial election in one of the states in Nigeria when the leading opposition party was alleged of planning to kit some thugs with police uniforms with the aim of snatching the ballot boxes and filling them with unlawful ballot papers. The ruling party later intercepted a vehicle, in the company of law enforcement agents, and after searching that vehicle, saw thumb printed ballot papers, just few weeks to the election.

Also, a raid was conducted on a public school where police uniforms and ballot papers already thumb-printed for the opposition party, as well as a lot of dangerous weapons were found. It is important to note that it was possible that the ruling party positioned some "straw men" (its agents) among the ranks of the opponent, collecting intelligence which can be used to monitor or identify the weakness of the opponent, or even implicate the opponent for the purpose of having strategic advantage over the enemy party;

n) Sex and Honey pots: How will you feel, if you found a poster or in the media, the picture of a deceased man whose family is announcing his demise, and in the course of the public announcement, it is said that the man died after having (marathon) sex? I know many people will burst into laughter considering the novelty or strangeness in the content of that announcement. This is because most families would rather put it as: 'he died after a brief illness'.

For better, for worse sex has remained one of the effective means of intelligence collection. Several kingdoms and empires have collapsed to the evils that sex is capable of evoking. In intelligence collection, sex is a very good tool of information sipping. The law enforcement agents use it to gather information, which can assist them in arresting some criminal suspects. Criminal suspects also apply it (sex) to get valuable information from security chiefs by trapping them with women particularly those men considered as 'women wrapper" (womanizers), to escape arrest by the law enforcement agents.

There are two basic ways that this technique can be facilitated: Internal and external. The external sources appear to be more effective than the internal. The external may include commercial sex workers, specific female members of the group (or agency, girl friends (or boy-friends) etc. The internal barriers may include one's spouse, and among those that commit incest, we may have daughters, fe(male) cousins, parent, mother(in-law) or father (in-law) among others.

The internal source(s) usually has (have) emotional attachment to the target person(s) which can make it a great risk using the internal sources for intelligence task. This is because, there is the tendency for such people to give false information (due to the bond or blood ties they have with the target persons, although there are some exceptions. The external sources appear to be more productive in intelligence collection, due to the unscrupulous nature of the relationship between the target persons and their sex partners. The basis for such relationship may only be material concern or mere canal pleasure or clandestine reporting etc; and

o) Walk-ins: Walk-ins also play great role(s) in intelligence collection. Walk-ins are those that voluntarily give information to law enforcement agents. But, it is quite important to know that the information must be subjected to scrutiny and analysis to know if such information is aimed at assisting the security operations in the combat of crime or meant to deceive security personnel.

SELF ASSESSMENT EXERCISE

Explain various means through which intelligence can be gathered.

4.0 CONCLUSION

Intelligence collection is that art and science of information gathering for intelligence activities. In an attempt to carry out investigation, there is need for security personnel to consider utmost means to gather information that will assist in crime detection, and even prevention of act(s) that can constitute a threat to national security e.g. terrorism, insurgency etc. Therefore, intelligence is not only collected to detect crime and identify the offender, but also to prevent crime and insecurity. The intrusive nature of intelligence collection has become a subject of (great) debate. This is because most intelligence information is collected in methods that can undermine the right to privacy of individual(s). Some of the means through which intelligence is collected have also brought up the moral question. This is because they are capable of undermining the fundamental rights of the people. It is therefore necessary to put in place control measures in the collection of intelligence.

5.0 SUMMARY

In this unit, we have been able to cover a wide spectrum of issues in discussion of the subject of intelligence collection. We began our academic journey into the subject (of the day) by considering some of the available definitions of intelligence collections for conceptual purpose(s). Thereafter, we focused on various disciplines of intelligence collection. The third (and last) area of discourse was the means of intelligence collection. I strongly believe that you have found this unit interesting.

6.0 TUTORED MARKED ASSIGNMENT

i. What is intelligence collection?
ii. State any four intelligence collection disciplines.
iii. List any four means of intelligence collection

7.0 REFERENCES AND FURTHER READING

Cline, L. E. (2005). *Pseudo Operations and Counter Insurgency: Lessons from other Countries*. Carlisle Barracks, PA: Strategic Studies Institute.

Hannah, G., O'Brien, K.A & Rathmell, A. (2005). *Intelligence and Security legislation for Security Reform*. Technical Report for the UK's Security Sector Development Advisory Team. Cambridge, UK: RAND Corporation.

Monahan, T. (ed.) (2006). *Surveillance and Security: Technological Politics and Power in Everyday life*. New York: Routledge.

Silverstein, K. (2007). Sex and the CIA. *Harpers Magazine*. (April 17). Also available on .harpers.or/archive/2007/04/sb-sex-and-the-cia. Retrieved on 1 January, 2008.

The US Dept of Defense (12 July, 2007). Joint Publication 1-02 Dept of Defense Dictionary of Military and Associated Terms. Available on .cia.gov/library/ center-for-the-stydy-of-intelligence/kent-csi/docs/vo8ila02p-0002.htm. Retrieved on 8 January, 2008.

.en.wikipedia.org.wiki/black-Black-Bag-Operations. Retrieved on 7 April, 2008.

.en.wikipedia.org/wili/intelligence-collection.Retrieved on 7 April, 2008.

://www.fas.org/irp/program/masint.htm. Retrieved on 6 March, 2008.

.militera.lib.ru/reseaech/suvorov8/16html. Retrieved on 4 April, 2008.

UNIT 3

INTELLIGENCE ANALYSIS AND EVALUATION

CONTENTS

7.0 References / Further Reading

1.0 INTRODUCTION

Collecting information for intelligence purpose(s) is not sufficient enough for it to become intelligence product. This is because, it is not all information gathered that will have equal importance in intelligence–planning. Some information may even be totally discarded for lack of merit. Then, how do we identify information that are important and those that are not? Well, in the intelligence community, the process of identifying those information that are relevant for one intelligence initiative or the other is effected by analysis. Therefore, the process of analyzing intelligence is very crucial in determining the quality of intelligence products. Here, there is application of knowledge in the evaluation of the collected information, which are refined and made useful for (Security) intelligence. In furtherance of (our) discourse on intelligence, and our attempt to show how it impacts on security practice and management it is important in this unit to illuminate on how intelligence analysis is done.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Define the concept, intelligence analysis;

Explain the pillars of intelligence analysis; and

Discuss steps in intelligence analysis.

3.0 MAIN BODY

3.1 Defining Intelligence Analysis

This is the process of determining out of available information, the ones that are useful in producing intelligence. The truth is that it is not all information gathered for intelligence will be useful, particularly as they relate to human nature analysis. It can also be described as:

---the process of taking know information about situations and entities of strategic, operationally or tactical importance, characterizing the known, and with appropriate statements if probability, the future actions in those situation and by those entities. The descriptions are drawn from what may only be available in the form of deliberately deceptive information; the analyst must correlate the similarities among

deceptions and extract a common truth (.en.wikipedia.org/wiki/Intelligence_Analysis).

---*a way of reducing the ambiguity of highly ambiguous situations, with the ambiguity often very deliberately created by highly intelligent people with mindsets very different from the analysis* (.en.wikipedia.org/wiki/Intelligence_Analysis).

However the services of knowledgeable persons are often required for intelligence analysis, considering the task of revealing the facts from available information, often through systematic evaluation or assessment. As you are expected to know, dealing with human-beings, one needs to be mentally alert. This is because man can be sometimes mischievous and will try to hide the truth by giving false information.

As a security operative, you need to be very vigilant. There is no doubt, (effective) intelligence analysis is generally missing in our security sector in Nigeria. May be, that is one of the factors responsible for ineffective security management. This also explains the problem of incapacitation of various security agencies to provide substantial evidence (criminal intelligence) in the prosecution of suspects. One of the examples of such inefficiency was displayed in the decision of the Lagos State High Court to discharge and acquit former chief security Officer to the Late Head of State, General Sanni Abacha, of the allegation of trying to overthrow the government of the erstwhile president Olusegun Obasanjo (1999 to 2007), for lack of evidence to show that the accused person committed the offence in actual fact.

Moreso, the Nigeria Police is also bedeviled, in its operations, with the problem of ineffective intelligence analysis or intelligence misanalysis. The second problem is very fatal, having security personnel acting on information without considering the merit of the less professional men and officers of the police institution show that the recruitment process(es) in the appointment and placement of people into its fold is (are) questionable. Do you know how many innocent people have been killed, maimed or wrongly prosecuted by the police in Nigeria?

I directly had a chat with one policeman, who told me that they shot some young men to death at the back of their station. The policeman informed me that an elder brother to one of the guys visited the police station, and reported that he suspected his younger brother and his friends of being armed robber. He asked the police to swing into action. Though, the action of the police to raid the target place was commendable but later actions were unprofessional and criminal. They searched the whole place, and found some incriminating objects like arms and ammunition. Thereafter, the young man who was reported by his brother as well as other friends and visitors were taken to the station. The suspects pled innocence of armed robbery to the police. In a regular extra-judicial jingoism and killing by most security personnel in Nigeria, the boys (suspects) were brutally murdered by the police personnel in question.

One fact which must be noted here is that the police agents failed to do their job (investigation) as demanded by the law while in exchange of fire should be in self-defense, and shooting to death any suspects (or convicts) can only be ordered by the court (of competent jurisdiction). The concerned police staff that carried out that dastardly act failed to subject the information given to them by an elder brother to one of the slain victims (suspects), to critical analysis to determine if the information was genuine or deceptive. Now, just imagine a situation where two brothers are fighting each other over the property left by their late father (or mother), and the elder one looking for a means to cheat his/her younger one while the younger one is resisting his/her brother's (or sister's) attempts. Hence, in a situation of conflict between the two, particularly when the elder one is greedy things may take any dimension. The conflict may involve the use of thugs or supernatural attacks or even clandestine tactics such as the use of hired killers, set-up etc.

What I have gathered from my inquiry is that the policemen failed to build any scenarios about the information they were about to act on. Even, after arresting those boys, one would expect them (the police) to take time in investigating the matter. They only swung into the killing of the boys without ascertaining their guilt (or innocence). What a barbaric way of security management! By and large, analysis is a very vital element of intelligence planning and production. The technical nature of this process demands that resourceful and intelligent people should be in charge of intelligence analysis. Anybody can be mandated or employed to collect information but the work of intelligence analysis is special and can only be managed by competent people who have intuition and insight.

It is not surprising, due to the importance of intelligence analysis in security management and crime detection and prevention, that a number of countries have specifically created schools to teach and impact (on) the people the skills of intelligence analysis. One of such schools is Mercy-Hurst College Institute for Intelligence Studies. Even several intelligence agencies have training centres for developing or improving among other things the skills of (a number of) their intelligence officers in intelligence analysis. A good example is Directorate of Intelligence (DI), a subsidiary of the US Central Intelligence Agency (CIA).

SELF ASSESSMENT EXRCISE

Define the term intelligence analysis.

3.2 Pillars of Intelligence Analysis

As I have mentioned earlier (in the last segment of this unit), analyzing intelligence is a very challenging task. This is because the analysts are confronted with a number of issues that can affect the outcome of the analysis. One of such factors that mitigate or undermine intelligence analysis is value. Value tends to create identity and imaging in the mind(s) of (any) analysts. In sharply ethnically divided countries like Nigeria, the probability of having distorted intelligence analyses will be high. This is because ethnicity often creates the problem of identity and (enemy) imaging in the minds of people. This problem covers all professions, segments and classes in Nigerian society, including ruling elites and security personnel. “No be your brother dey for government” (is it not your brother who is in government? has become a regular phrase in Nigeria by which people express their opinion(s) about one regime or the other based on ethnic identification. So, a situation like this gives ethnic legitimation to political leadership. Thereby, the shortcomings of any political leader are ascribed to his/her ethnic group.

However, it is pertinent for intelligence analysts to avoid those turning their back or the pillars of intelligence analysis, which are the factors that can promote effective intelligence analysis, and these include:

a) Boldness and Honesty: Honesty, they say, is the best policy. It is expected that for effective discharge of his/her duties, an intelligence analyst must not only be honest but must also show to be honest. Analyst should not allow some extraneous variables or selfish motives affect his/her job. And in maintaining honest posture and resilience against distortion of facts, analyst will need to be bold, thus:

> *…believe in your own professional judgments. Always be willing to listen to alternative conclusions or other points of view, but stand your ground, if you really believe the intelligence supports a certain conclusion. Just because some is your boss, is higher grade, or has been around longer than you, does not mean he or she knows more about your account than you do. You are the one who reads the traffic everyday and who studies the issue --- It is better to be mistaken than wrong* (Watanabe, 1997).

Reflecting on the last statement “It is better to be mistaken than wrong” in the above comment made by Watanabe, you may agree with me that the fear often exhibited by policy makers, from being found wrong in the choice of policy options, usually accounts for the ill-advice they get here and there. It is unfortunate that these ill-advices, most times influence their policy direction(s). Therefore, it is important for policy makers to have intelligence advisors and there should be significant amount of trust in their relationship. Also, the intelligence advisors are advised not to misinform the policy makers or the executive whom they are working with for any reasons, and there must be honesty;

b) Goal Setting: This is a crucial aspect of intelligence analysis. It is paramount to the goals the intelligence consumer as well as needs of the consumer (like government, corporate organization etc). And it is most important to complement what the consumer has with the knowledge of intelligence being analyzed. It is by doing this that you will be able to reconcile and synthesize various information available to you, and bring out those which the consumer does not have any previous knowledge of but can also meet his/her overall goal agenda;

c) Appreciating the Consumer's View and Expectations: It is important for analysts to appreciate the views and expectations of the consumer(s). Sometimes, you may prepare intelligence for a particular consumer or the other, but are further requested to provide intelligence that is more detailed than the one you brought. For instance, you may prepare intelligence based information gathered by human sources (HUMINT) but your customer may ask you to provide a more detailed one which may require considering other sources like imagery intelligence (IMINT), signal Intelligence (SIGINT) etc.

   As an analyst, you need to comply with your customer's demand and make sure that intelligence is produced in a very interactive and self explanatory way, such that the customer will find it easy to understand. Therefore, you need to consider the educational background of your customer, and simplify the technical words to carry him/her (customer) along;

d) Organization of Information Available: Analysts get a lot of information from various sources of intelligence collection. It is the job of an analyst to identify the information that are important and those that are not, to the task before him/her. He/she should also ensure that information that are true should be separated from false ones. In some intelligence institutions, information are sorted or arranged with the use of standard code according to the probable worth of confidence of the information and its collection source.

   The intelligence analysis (IA) professional is confronted each day with high demands for rapid, yet accurate assessments that require discovery and marshalling of evidence, integration and synthesis of data from disparate sources, interpreting and evaluating data and information that are constantly changing, and making recommendations or predictions in the face of inconsistent and incomplete data (Greitzer, 2005: 1). In addition, after organizing the information, the process of evaluation will take place to assess the value of each of the information and the analyst will come up with some hypotheses; and

e) Team playing: An analyst needs to demonstrate at least a minimum degree of partnering with some other team players in the field. He/she should not see them as rivals but should regard them as colleagues. It is only when this is done that he/she can work with others conveniently. Therefore, analysts need to adequately motivate the intelligence collectors who provide them with information to carry out their work. As an analyst, you need to always appreciate the work of the intelligence collectors and endeavour to feed them back. This is because "if you are not frequently tasking collectors and giving them feedback on their reporting you are failing to do an important part of your job" (Watanabe, 1997).

SELF ASSESSMENT EXERCISE

Explain the pillars of intelligence Analysis

3.3. Steps in Intelligence Analysis

There are various steps, which analysts take in the discharge of their official duties–to analyse intelligence. Though, there is no consensus on any particular process to be adopted by analysts. They often adopt different approaches not only in the collection but also in the analysing of intelligence. Nonetheless, various steps in the process of intelligence analyses may include:

a) Definition of the Problem: analysts will need to seek and know the questions in the minds of their customers which bother on their intelligence requests. If the questions are unclear the analysts will need to demand for further clarification to illuminate the thinking of the customer;

b) Developing Hypotheses: Hypotheses are statements, which are developed to predict the relationship between two variables. For instance, if you have a customer who is one of the major players in the banking industry of the country to provide intelligence on how she can attract people to her loan facilities, you are likely to come up with some statements (hypotheses) like these:

   (i) The lesser the rate of a loan facility, the higher it becomes attractive to people (customers and prospective customers);
   (ii) The lesser the conditions attached to accessing a loan facility, the more people will get attracted and seek for loan from the bank; and
   (iii) It is better to concentrate more on low income earners than high income earners considering their population. Etc.

   Analysts generate hypothesis by tasking their brains to identify various probable variables, which can have impact on addressing the problem of the intelligence sought by the customer;

c) Data Collection: Analysts require information to do their work. In the case of not having information already the analyst requests for the services of human intelligence collectors like spies or agents. They also rely on other sources of data collection like communication interception and satellites. But these tasks (of intelligence collection) are carried out by intelligence collectors. Sometimes, analysts rely on information gotten through newspapers, public records or archive etc;

d) Evaluation of Information (sources): Analysts should have an assessment test on the information available to him/her and the sources of such information. This is because distortion of information or deception cannot be ruled out in data collection. It is therefore important to evaluate how accurate each information is, through which you identify those that are useful and those that are not;

e) Evaluate (Test) Hypotheses: This is the most crucial stage of intelligence analysis. Analysts should ensure that they carry out a comparative analysis between the gathered evidence and their formulated hypotheses, with the application (or use) of different analytical tools and methods like Analysis of competing hypotheses etc. This process will enable us to identify the hypotheses that are not useful or which are irrelevant, which may be thrown out;

f) Production and Packaging: After evaluating the hypotheses, analyst will come up with (intelligence) findings which he/she considers in packaging the intelligence product. In the production of intelligence, three issues usually come to bear, and these include:

> Timeliness: Timeliness includes not only the amount of time required to deliver the product, but also the usefulness of the product to the customer at a given moment.
>
> Scope: Scope involves the level of detail or comprehensiveness of the material contained in the product; and
>
> Periodicity: Periodicity describes the schedule of product initiation and generation (**Error! Hyperlink reference not valid.**)

Intelligence product is packaged either by written presentation, oral or electronic presentation (or both). In some organizations, request is made for intelligence by demanding the analyst to present the product in written and oral forms;

g) Peer Review: There is the general belief that two heads are better than one. After the production of intelligence, it is advisable for analysts to seek for comments from their colleagues in the intelligence community who may identify area(s) of deficiency in the intelligence product. This view is also shared by the United States Department of Defense (DoD):

> *Coordination with peers is necessary…..if you think you are right and the coordinator disagrees, let the assessment reflect that difference of opinion and use a footnote, called a reclama* (.dtic.mil/doctrine/jel /new pubs/jp102.pdf).

Exchange of ideas is very essential in the production of intelligence. As an analyst, there may be some flaws, which you may not identify, but bringing on board some other colleagues of yours in the intelligence business, may alert you about such flaws or errors. You must also be humble enough to entertain criticisms and see how various comments made can be catalogued, ranked and applied to improve your intelligence product. Also, as an analyst you should always have it at the back of your mind, that no man is an island (of knowledge). For this reason, it is important that one should choose among his/her colleagues those to work with as a team. In this case good human relation and trust-building are essential; and

h) Customer Feedback and Production Evaluation: After delivering the intelligence product to your customer, you are also expected to always meet your customer and ask question about the product. The questions may include: Has the intelligence been effective enough or useful in meeting the customer's goals? Does the customer find the intelligence product easy to use? etc. Analysts and their customers (policy makers, corporate organizations, individuals, security agencies etc) must make regular contacts to discuss the efficacy or ineffectiveness of the intelligence products with the aim of fathoming ways to refine and put more life into them (intelligence products). By doing these, it will be easy to meet the expectations of the customers.

SELF ASSESSMENT EXERCISE

How do you explain various steps to be undertaken in the production of intelligence?

4.0 CONCLUSION

Intelligence analysis is the process of putting information in the right perspective by removing those information that are not useful as well those that are distorted or false in intelligence planning and production. It is a very technical aspect of intelligence work which demands that anyone who wants to undertake such task should demonstrate high sense of intelligence and must be knowledgeable.

The analysts usually apply some specific methodologies in the conduct of intelligence analysis and they're often referred to as analytic tradecraft. In the business of intelligence analysis, you are expected to understand the nature of the business by professionally identifying the needs of the customer and the questions he/she want to solve with the use of your intelligence product. Therefore your product must be problem-solving by providing the customer with an array of options that he/she can use to meet his/her goals.

5.0 SUMMARY

In this unit, we have been able to look at a wide range of issues concerning the subject matter: intelligence analysis. We set out in our academic adventure by first explaining the meaning of intelligence analysis. Thereafter, we highlighted the various pillars of intelligence analysis. The last area of inquiry was the various steps of intelligence analyses. Thank you for your attention.

6.0 TUTORED MARKED ASSIGNMENT

(i) What is intelligence analysis?
(ii) Explain steps in intelligence analysis.

7.0 REFERENCES AND FURTHER READING

Central intelligence Agency, Directorate of intelligence (Feb, 1997), A Compendium of Analytic Tradecraft Notes; .au.af.mil/au/awc/awcgate/cia/tradecraft_notes /contents.htm. Retrieved on 23 of October 2007.

Davis, Jack (1995), "A policymaker's Perspective on Intelligence Analysis", Studies in Intelligence, No 5. Also available on .cia.gov/library/centre-for-the-study-of-intelligence/csi-publications/csi-studies/studies/95unclass/Davis.htm. Retrieved on 23 October, 2007.

Greitzer, F.L. (March 2005), Methodology, Metrics and Measures for Testing and Evaluation of Intelligence Analysis Tools, Pacific Northwest Division of Battelle Memorial Institute.

Heuer, Richard J. Jr. (1999), Psychology of Intelligence Analysis Chapter 8: Analysis of Competing Hypotheses, available on .au.af.mil./au/awc/awcgate/psych-intel/art10.html. Retrieved on 23 October, 2007.

Johnston, R. (2003), "Developing A Taxonomy of Intelligence Analysis Variables". CIA: Studies in Intelligence, 47(3). Available on ://www.cia.gov/csi/studies/vol 47no3/article05.html. Retrieved on 24 October, 2007.

Krizan, Lisa (June 1999), Intelligence Essentials for Everyone. Washington D.C: Joint Military Intelligence College. Also available on .scip.org/2_getintel /ess.php. 2 October, 2007.

US Department of Defense (12 July 2007), Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms. Available on .dtic.mil/dotrine/jel/new_pubs/jp1_02.pdf. Retrieved on 1 October, 2007.

Watanabe, F. (1997), "Fifteen Axioms for Intelligence Analysts: How to Succeed in the DI {Directorate of Intelligence}", *Studies in Intelligence*. Available on .bss.sfsu.edu/fischer/IR%20360/Readings/15%20axioms.htm. Retrieved on 23 October, 2007.

.en.wikipedia.org/wiki/Intelligence_Analysis. Retrieved on 20 April, 2008.

UNIT 4

COUNTER-INTELLIGENCE

1.0 INTRODUCTION

In the last three units our focus has been drawn to the meaning of intelligence, intelligence collection and analysis. Every nation usually develops mechanisms and establishes institutions that engage in intelligence activities while assisting her to have strategic relevance in the world polity. In achieving the overall security agenda, nations don't only focus on how various intelligence activities can enhance their internal security, but also consider very importantly creating measures and platforms that can counter any intelligence (or security) threats emanating from both local and external enemies which are capable of undermining their national security.

It is against this background that counter-intelligence has become a key element of security planning and management. Counter-intelligence is part of intelligence cycle and its coordination must also include the security issues that bother on protection of intelligence personnel, their facilities as well as operation. These shall form the bases of this unit. Now, let's quickly browse through the objectives of this unit.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Define counter-intelligence;

Explain aspects of counter-intelligence; and

Discuss protective disciplines for counter-intelligence.

3.0 MAIN BODY

3.1 **Definition of Counter-Intelligence**

Counter-intelligence (CI) has become a rapidly growing intellectual area of inquiry in security studies. It enables us to appreciate the need to look at intelligence from a dual perspective: our strengths and vulnerabilities or weaknesses. It is only when we can identify our weaknesses that we can fathom ways through which we can secure our intelligence community and counter other security threats. On the definition of counter intelligence, we can consider the following:

Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted for by or on behalf of foreign government or elements thereof, foreign organizations or foreign persons, or international tourist activities (see .fas.org/sgp/crs/intel/RL33616.pdf).

Counterintelligence (CI) refers to efforts made by intelligence organizations to prevent hostile or enemy intelligence organizations from successfully gathering and collecting against them. Many governments organize counter-intelligence agencies *separate and distinct from their intelligence collection services for specialized purposes* (see .en.wikipedia.org/wiki/counter-intelligence).

According to the United States Army in its manual on counter-intelligence, our conceptual definition of counter-intelligence cannot be complete, if we fail to consider two basic tasks performed by counter intelligence in our conceptual clarification of the term, CI. And these include:

- Developing, maintaining, and disseminating multi-discipline threat data and intelligence files on organizations, locations, and individuals of CI interests. These include insurgents and terrorist infrastructure and individuals who can assist in the CI mission; and

- Educating personnel in all fields of security. A component of this is the multidiscipline threat briefing. Briefings can and should be tailored, both in scope and classification level. Briefings could then be used to familiarize supported commands with the nature of the multidiscipline threat posed against the command or activity (US Dept of the Army, 1995).

However, in several countries intelligence services are given separate mandates, and therefore counter intelligence institutions operate independently of other intelligence agencies. For instance, in Britain, there exists an independent security organization known as “security service” or “MI-5, having no police powers but is mandated by the law to have a good or collaborative working relation with the law enforcement agency known as the “Special Branch”. MI-5 performs counter-intelligence functions and through the special Branch, she can effect arrest or interrogate or facilitate a search warrant (on) suspected enemies or intelligence threats.

In the United States, the Federal Bureau for Investigation (FBI) appears to be the major counter-intelligence agency in the country. In Nigeria, there is no clear cut separation of functions among the intelligence agencies in the country. What I mean is that there is no actual intelligence organization that is basically mandated by the law for counter-intelligence only.

3.2 Aspects of Counter-Intelligence

In this segment of the unit, we are going to look at various aspects of counter intelligence, though, there may be more aspects than the ones we are providing in this study due to the dynamics of counter-intelligence activities and studies. That notwithstanding, we shall be focusing on four major aspects of counter intelligence. These include:

a) Defensive counter intelligence: This aspect draws its attention from identifying vulnerable areas in one’s intelligence organization(s) which can be explored by foreign intelligence services (FIS). The term, FIS in (modern) counter-intelligence goes beyond foreign countries or agents in its meaning. It simply refers to ‘any opposition’ (in security terms not politics), either internal or external.

Defensive counter intelligence activities should cover defending one’s nation or organization against any threat that can undermine its security as well as protecting the friendly nation against enemy’s attack, which may be as a result of the diplomatic support your nation enjoys from the friendly nation, making the enemy-party dissatisfied. In one of the broadcasts made by Osama bin Laden, the leader of Al Queda network, he called on the members of his group and his sympathizers (lovers) to carry out insurgent actions to destroy the United States and its allies.

This explains some of the covert support being received by some local insurgents in a number of countries from Al Queda network, to fight their governments who are considered to be Pro-West by Al Queda and the like. The Pro-American posture of the Iraqi government (majorly controlled by Shiites) has attracted insurgent condemnation not only from the Sunni dissidents but also violent threats from the Shiites militants.

The Shiites insurgency in Iraq has added a new twist to the post-war Iraq discourse. This is because most people would think having a Shiite led government, the majority Shiite population would welcome it and give her the necessary support to succeed. But the case has turned out to be contrary, resulting from the fact that more aggression comes from the Shiites rather than the Sunnis.

Well, one important revelation is that the aggression is more likely to be sponsored by Iran in evoking its defensive counter-intelligence, considering the threat in the US sojourn in Iraq could constitute against its national security. The covert support, Iran gives the Shiite insurgents in Iraq is overwhelming, with the aim of forcing the US and allies to consider the option of leaving Iraq. If this is achieved by Iran, the US will not have access to Iraq as its military base through which it can launch a military invasion of Iran, in stopping her (Iran) from further developing nuclear power or any others weapons of mass destruction (WMD);

b) Offensive Counter intelligence Operations: These include all activities that are targeted towards arresting the mischief of the enemy-parties. It is important to put in place measures that will undermine the structure and personnel of hostile intelligence organizations (Wisner, 1993). This aspect is also known as counter espionage. Here, efforts are made towards identifying and arresting the agents of a foreign intelligence services or enemy parties. If the hostile agents are diplomats, the friendly nation or host country should declare them *persona non grata*, and facilitate their immediate repatriation. The hostile agents who are not diplomats are to be arrested by law enforcement agents, and be prosecuted. In some countries, if a spy is caught within or outside their intelligence domains working for foreign interests, he/she usually faces highest penalty (death sentence) while some other countries only have them imprisoned.

Intelligence services can also subject the detained hostile spies to torture, forcing them to reveal their planned clandestine actions for the purposes of liquidating such plans and prevent similar threats from any other hostile spies in the nearest future. Recently, the Nigerian government through its security operatives arrested some people alleged to be foreign spies and their local co-conspirators who were accused of espionage;

c) Counter-intelligence Protection of Intelligence Services: Intelligence services don’t only guard the states) against external infiltrations and (internal) attacks but also undertake some (defensive) counter-intelligence actions or measures to protect against attacks or threats from the enemy or hostile party(ies). Therefore, there is need for intelligence agencies to evaluate the source of, methods and resources they use in intelligence activities. There is also the need by intelligence services to conduct risk assessment on its operations with a view to identify appropriate counter-intelligence measures to the risks in its operations; and

d) Counterintelligence Force Protection Source Operations (CFSO): These involve human source operations in which Clandestine activities “are conducted abroad…..intended to fill the exiting gap in national coverage, as well as the combatant commander’s intelligence requirements” (**Error! Hyperlink reference not valid.**; and US Dept of the Army, 1995).

SELF ASSESSMENT EXERCISE

Discuss aspects of counterintelligence.

3.3 Protective Disciplines and Counter-Intelligence

These disciplines don’t actually have any direct relationship with intelligence activities but only play some complementary roles. They assist to reinforce counterintelligence measures to undermine enemy’s attacks on the intelligence community and nation at large. They include the following:

a) Physical Security: It is the duty of intelligence services to ensure protection of their physical infrastructure against attacks of enemies that operate within and outside. Apart from that, efforts are made to secure the civilian and government facilities against infiltrations and attacks from mischievous elements (or foreign intelligence services). Infrastructures like building require measures than can counter any threats the enemies can make use of tall buildings; after gaining access to it, to monitor the movement of the occupants of another building being targeted.

Consequently, after collecting intelligence, enemies might identify the vulnerable areas, and strike. This can also explain the tactics adopted by the Al Qaeda network in the planning and execution of the carnage (Sept 11 incident) that visited the United States. The terrorists studied the US and its geography, noticing that there had been tight security at its borders making it difficult to smuggle in explosives into the country, so, they chose to hijack commercial aircrafts and hit them against target building(s). The US intelligence community failed to mount adequate surveillance on the Arab immigrants who pretended to be students and enrolled to study piloting.

Physical security may also include fortifying infrastructures and building with security gadgets and other measure like the use of window blind. The use of window blinds will prevent activities in the room from being seen through the windows. Intelligence facilities need to be protected by putting in place high construction standards that are capable of mitigating enemy’s attacks and ‘might slow down, but certainly not stop, a determined entry attempt that used explosives’ (.en.wikipedia.org/wiki/Counter-intelligence);

b) Personnel Security: Sometimes foreign intelligence services use some of the trusted people in an organisation or state to unleash their terror or attack. FIS can decide to buy over some of the people working for your organization or home government who have access to some secrets that may be useful to FIS. In order to avoid a situation like this, intelligence services will need to put in place security clearance system (or positive vetting) to ascertain if a person within the organization, holding sensitive position can still be trusted or not.

The services will have to conduct periodic clearance on the people holding sensitive or strategic positions. One of the ways to do this is secret monitoring of their spending against his/her their income. If one spends far above his/her legitimate earnings, such person needs to be scrutinized. There must be electronic reviews of one’s financial records, and it is also important to examine the lifestyle of each staff to identify the areas of vulnerability of each of them, and apply measures that can limit or curb possible compromise among (the) personnel;

c) Operations Security (OPSEC): This underscores the relevance of information, which is very crucial to the future operations of any organization or country, and, how ‘planning activities’ should be shaped to:

- ❖ Identifying those actions that can be observed by adversary intelligence systems;

- Determining indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and

- Designing and executing measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation (see .en.wikipedia.org/wiki/intelligence-cycle-secur ity).

Operations security usually involves taking some measures like counter imagery, cover, concealment and deception to identify the interests and needs of the adversary in its (hostile) relation towards the friendly service (or country) as well as discovering critical clues about the services, which the enemy can collate, analyze and synthesize for (strategic) intelligence viewpoints, which can be used to identify or detect the vulnerabilities of the friendly service in its desires to carry out its threats. It is therefore, necessary to develop measures that can mitigate the enemy's threat by adequately addressing the problem of vulnerabilities being encountered by the friendly service; and

d) Communication Security (COMSEC): This is also germane to counter-intelligence. In intelligence activities, communication plays a great role, and that is why both the friendly service and enemy often extend their intelligence aggression to communication (environment). Therefore, security of one's communications and interception of the enemy's has become one of the foremost principles in intelligence community (IC). Communications security is geared towards:

> *…preventing an adversary to intercept sensitive information that is transmitted, especially through free spaces, but also through wired networks capable of being wiretapped. It includes several disciplines, both including those for protecting the hostile acquisition of information either from the patterns of flow of messages, or the content of messages..* (see .en.wikipedia.org/wiki/intelligence-cycle-security).

Communication security is a key element of counter-intelligence. That is why it is essential for security organizations including the military, to provide secure communications and guard against interception by the FIS (or enemies). Some of the counter-measures against any specialized technical interception from the enemy may include encryption, traffic flow security, steganography etc. The intelligence services are also expected to shield their office buildings against any electronic attack

SELF ASSESSMENT EXERCISE

Discuss the protective discipline for Counter-intelligence

4.0 CONCLUSION

Counter-intelligence activities have become widened in recent time due to emergent (non-traditional) security threats that characterize national and international politics. In the olden days, security threats emanated from another country but now local dissidents constitute the greatest security threats, undermining national security, many of whom are even working for foreign interests. Compromise (to enemy's influence) has become a major challenge in intelligence community in which intelligence officers sell (or give) classified information or secrets of their services (employers) to Foreign Intelligence Services (FIS).

The level of sophistication of modern communication technologies has also made friendly intelligence service vulnerable to technical interception and attacks of the enemies. These and other factors have necessitated the need to put in place measures by intelligence community, to mitigate (reduce) or prevent threats from enemies. Counter-intelligence activities should ensure not only to counter the attacks coming from the enemies but also to protect intelligence personnel, facilities, resources as well as operations. It is by doing all these that effective counter-intelligence can be actualized.

5.0 SUMMARY

In this unit, we have been able to discuss a number of issues as regards counter-intelligence. We began our intellectual discourse by looking at some of the available definitions of the term, counter-intelligence, in the actualization of our task of conceptualization. Thereafter, we explained various aspects of counter-intelligence. The third and the last subject we treated was the list of major protective disciplines for counter-intelligence.

6.0 TUTORED MARKED ASSIGNMENT

What is counter-intelligence?
How do you explain various protective disciplines for counter-intelligence?

7.0 REFERENCES AND FURTHER READING

Archick, K. (2006). European Approaches to Homeland Security and Counterterrorism. Congressional Research Service (CRS Report Number: RL33573). (July 24). Also available on .fas.org/spg/crs/homesec/RL33573.pdf. Retrieved on 5 November, 2007.

Dulles, A. W. (1977). *The Craft of Intelligence*. Westport, CT: Greenwood.

Imbus, Michael T. (April 2002), Identifying Threats: Improving Intelligence and Counterintelligence Support to Force Protection. See .au.af.mil/au/awcgate/ acsc/02-059.pdf. Retrieved on 3rd Nov. 2007.

US Department of the Army (3 October 1995), Field Manual 34-60: Counterintelligence, available on .fas.org/irp/doddir/army/fm34-60. Retrieved on 5 November, 2007.

Van Cleave, Michelle K. (April 2007), Counterintelligence and National Strategy, School for National Security Executive Education, National Defense University (NDU).

Wisner, Frank G. (22 Sept. 1993), On "The Craft of Intelligence", available on .cia.gav/library/center-for-the-study-ofintelligence/Kent-CSI/doc/V081a07p-0004.htm. Retrieved on 3rd November, 2007.

.en.wikipedia.org/wiki/Counter-intelligence. Retrieved on 4 April, 2008.

.en.wikipedia.org/wiki/intelligence-cycle-security. Retrieved on 5 April, 2008.

.fas.org/spg/crs/intel/RL33616 .pdf. Retrieved on 5 April, 2008.

UNIT 5

DATA MINING AND AUTOMATED DATA ANALYSIS

CONTENTS

1.0 INTRODUCTION

In this unit, we shall be drawing our attention to the subject, Data Mining and Automated Data Analysis in furtherance of our study on basic security tools and applications. These concepts are relatively new in security studies and practice. They are inter-related and complementary because two of them are two sides of the same coin. Data mining and Automated data analysis have continued to attract robust acceptance and appreciation not only among security practitioners but also corporations or commercial ventures that often use these tools to improve their businesses. It is my belief that you will find this unit intellectually rewarding. Meanwhile, in the following segment of this unit, we shall quickly go through various tasks we hope to accomplish in this unit.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

Explain the meaning of data mining;

Describe automated data analysis; and

Discuss the application processes for data mining and automated data analysis

3.0 MAIN BODY

3.1 Meaning of Data Mining

As earlier stated in the introductory segment of this unit, data mining and automated data analysis are inter-related as two of them play complementary roles in intelligence reporting as well as in security investigation. No doubt, they are very effective tools and applications in crime prevention and detection. They can help to unravel secrets in organised crimes like terrorism, assassination, computer intrusion, theft, financial fraud, armed robbery, electoral malpractices, money laundering, among others.

Alas, these two concepts can be less effective or absolutely defective, if we fail to understand effectively well their guidelines and controls. It is therefore advisable for security professionals and policy makers to always "....acquire an understanding of data mining and automated data analysis tools so that they can craft policy that encourages responsible use and sets parameters for that use" (DeRosa, 2004: v).

At this juncture, let us subject the concepts to conceptual illumination, but in this segment, we shall begin with data mining. So, what is data mining? It is worthy to note that data mining is also known as Knowledge-Discovery in Databases (KDD) (see ://www.wisegeek.com/what-is-data-mining.htm).

As you may agree with me, one of the major features of Social Sciences and other related fields is the absence of universal definition of any terms among scholars. Social scientists define concepts not only according to their respective disciples but also from individual choice of perspectives. For this reason, we shall consider different definitions of the term data mining. Some the definitions of data mining include the following:

Data mining (sometimes called data or knowledge discovery) is the process of analyzing data from different perspectives and summarizing it into useful information ...Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases (://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm).

Data mining can also be described as:

....the process of extracting patterns from data. As more data is gathered, with the amount of data doubling........., data mining is becoming an increasingly important tool to transform this data into information. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and scientific discovery (://en.wikipedia.org/wiki/Data_mining).

Data mining can also be said to be a tool that makes use of:

......automated statistical analysis techniques....., discovering new trends and patterns of behavior that previously went unnoticed. Once they've uncovered this vital intelligence, it can be used in a predictive manner for a variety of applications (://databases.about.com/od/datamining/a/datamining.htm)

We can also contend that:

Data mining is usually defined as searching, analyzing and sifting through large amounts of data to find relationships, patterns, or any significant statistical correlations. With the advent of computers, large databases and the internet, it is easier than ever to collect millions, billions and even trillions of pieces of data that can then be systematically analyzed to help look for relationships and to seek solutions to difficult problems (://www.tech-faq.com/data-mining.shtml)

Data mining is also an application that:

......uses a relatively large amount of computing power operating on a large set of data to determine regularities and connections between data points. Algorithms that employ techniques from statistics, machine learning and pattern recognition are used

to search large databases automatically (://www.wisegeek.com/what-is-data-mining.htm).

SELF ASSESSMENT EXERCISE

What is data-mining?

3.2 Meaning of Automated Data Analysis

Automated data analysis can be described as a tool designed to:

...........find previously unknown knowledge through links, associations, and patterns in data (DeRosa, 2004: 3; Jensen, 2003).

Additionally, automated data analysis involves:

....the use of large databases containing identifying information assists in the important task of accurate identification (DeRosa, 2004: 6).

Automated data analysis can be applied in two ways, which include:

The use of subject-based queries; and
The use of pattern-based queries.

Subject-based queries: In subject-based queries, we begin data analysis with a particular and known subject, and continue the process by searching for more information about the subject. In this case, the subjects identity could be of a crime suspect, a religious leader, a security officer, a suspect at large, a bank official, a politician, to mention a few. In seeking to get more information about the subject, we may decide to probe his/her various contacts with other people, places, even telephone or/and communication facilities and other things that can assist us in our investigation, especially as it involves getting clues that can help us unravel some facts about the subject.

A subject-based query assists us in our analysis of data to have more information about the subject and gives us a clearer picture of what the subject is up to especially as it concerns his/her activities. This opportunity is attained through provision of (useful) link between the subject and other elements of our investigative scrutiny. Again, the beauty about this model is that it affords us an opportunity to identify other subjects that we will need to include in our investigation. One vital element of the subject-based query is link analysis. It helps to draw a connection between the subject and other subjects or places and things we will need to arriving at a decision in our investigation and analysis. Link analysis is usually popular among public security practitioners like the Police and intelligence agencies.

Meanwhile, in Nigeria, application of subject-based queries is very inadequate and ineffective because of the poor information infrastructure in public security sector. It is absolutely ridiculous in a country like Nigeria to have a police institution that does not have any computing system network that connects all its various stations and posts, area offices and state commands, as well as zonal/regional offices to the headquarters for proper record keeping of their activities and crime files (see Alemika, 2004; Shettima. & Chukwuma, 2002). The existence of central information system will enable all its offices to access and make information contributions to the database on suspects-profiling, prompt crime situation reporting, staff information and auditing, intelligence gathering and sharing, among others.

However, lack of technological innovation has really undermined the capacity of the police to perform its functions in Nigeria, a situation which has attracted the decision of most the state governors in the country to call for introduction of Joint Task Force (patrol team consisting of the police and men of the armed forces). Painfully, this is an indictment on the police authorities, for the failure of the police to live up to its responsibilities. Also, many people have claimed that several of the dismissed policemen have continued to find their ways back into the force without being detected by police authorities. For instance, a dismissed policeman might have been previously recruited in Lagos, and after his dismissal, he may proceed to Ondo state in an effort to be recruited into the Police again. The question that comes to one’s mind here is- if Nigeria Police fails to keep proper record of its personnel, how can it have adequate record of crime suspects? That means the police can hardly identify who is or not a first time offender except the suspect is well known by the officer in charge of the investigation.

Coming back to the subject matter, subject-based queries are potentially useful as forms of inquiries that characterise intelligence and law enforcement practice, which involve conducting a further search on the activities and relationships of the subject (someone under investigation) with other people. In this course of investigation, we may identify other people whose presence will be required to providing us a breakthrough and opportunity to have a successful investigation of the subject.

On the other hand, **pattern-based queries** involve conducting our investigation by moving from unknown to known. Here, we don’t actually have any subject on our minds but through a pattern of activity, we may decide to probe further into the activity that we suspect may constitute act of criminality or a threat to security. For instance, we may detect that through bank money transfers, some activities involving importation of expensive goods into the country are noticed. And if this same pattern of activity is noticed to be taking place from time to time, then, we can investigate the persons involved in such transactions. After identifying the persons, we may probe further to know if the subjects have strong and genuine businesses to warrant having large sums of money that they often transfer to purchase expensive goods abroad. Then, our pattern-based queries will change to subject-based queries because through the pattern of activity, we have identified some persons who were not previously in the picture and can be subjected to further scrutiny.

Thereafter, the suspected persons will become our subjects (those we investigate) and we will conduct further search on their activities and relationships. At the end of the day, after a thorough search and analysis, we may find out that the suspected persons are fronting for some public office holders who embezzle public funds and use it for their personal aggrandisement. Knowing that they cannot lodge such money into their private accounts, corrupt leaders tend to use some unsuspected persons to front for them through whom they use the money for all sorts of investment or property acquisitions.

SELF ASSESSMENT EXERCISE

How do you describe automated data-mining?
What are the two basic ways through which automated data analysis can be applied?

3.3 Application Processes for Data-Mining and Automated Data Analysis

Data-mining and automated data analysis are very important tools of security threat management as well as intelligence collection and analysis. Meanwhile, they require proper application and administration of various processes pertaining to their usage. It is therefore essential to have proper understanding of these processes in order to avoid making errors and information abuse. It is against this background that we shall be explaining in this segment, the steps to be taken in effective usage of these two concepts: data mining and automated data analysis.

a) Collection and Processing of Data: Collecting relevant data and useful information is a very big task. The reason is that it is more difficult to identify information useful for our task than the challenges we may encounter in the collection of data. It is always advisable to before we set out for the gathering of data, to always consider what we seek to achieve in our analysis, so that we will be able to conclude appropriately on the kind of information that will be useful to achieve the purpose of our investigation.

   There is no doubt that innovations in technology have made it easy to mine data (see Mostashari, 2003). Introduction of computing systems has really impacted positively on the task of data mining. Presently, through computer, we can develop a large database through which we can also create a single database for our data mining, a process known as data warehouse or data mart. We can also conduct our data mining by using a variety of database. For instance, if we are investigating a political office-holder accused of corruption, we may collate information through several means like conducting a search on all his/her official transactions and his/her contacts and relationships as well as financial transactions made by those with whom the suspect has one relationship or the other especially his/her family members.

Also, we can conduct a search on the private companies owned by the suspect including their various business and financial transactions as well as the activities of their respective management among others. If we consider the foregoing example, you may agree with me that data mining process is a difficult task that may involve the use of different databases in the collection of the needed information. After collating the information considered useful for our analysis, it is important to consider the standardisation and cleansing of the collected data so that we can identify which among the data, that can be most useful to our analysis task. By doing this, we shall be avoiding misuse of information.

According to DeRosa (2004: 10), the last step in this process involves "transforming the data to make them useful". This step is usually known as "data aggregation". It enables us to remove unimportant or unusable data by cleaning them, and the data are standardised for accuracy in our searches. By following these steps, we would reduce data errors that may mar our analysis especially errors like false positives and false negatives.

False positive errors are those errors that bother on the possibility of wrongfully labelling an innocent person as a crime suspect/criminal due to mistakes in the result of our automated data analysis. This error is usually associated with collection of wrong data or misapplication of data through imperfect search models (see DeRosa, 2004: 10). It will be improper to accuse innocent persons because they have relationship at one time or the other with any crime suspects or convicts due to inaccurate data mining or defective automated data analysis procedure.

On the other hand, in computer security, when a spam email is wrongly classified as non-spam email, we can therefore conclude that a **false negative error** has been committed (see ://www.cgisecurity.com/questions/false negative.shtml). Another example is if the result of our automated data analysis confirms a real crime suspect not culpable, meaning that our investigation effort is entirely faulty due to wrong check and defective data mining process and/or wrong procedure of analysis;

b) Finding Search Models: In carrying out our data analysis, we need a search model. For instance, if we want to use pattern-based searching, it will be cumbersome to get perfect models that help us to achieve good results in our automated data analysis. Meanwhile, we can adopt a "bottom-up" approach, using data mining to develop a model such that we search for anomalies or patterns that surround a behaviour or activity. We can also use "top-down approach" in analysing our data by beginning the process of analysis with a hypothesis "...about the model and determining whether it exists in data" (DeRosa, 2004: 11). By and large, models developed must be predictive and relevant to investigation. We should avoid running into the problem of data-dredging, resulting from models that are poorly designed; and

c) Decision making: The decision making process is also very significant in the application of data-mining and automated data analysis. It is the climax of the data-mining and automated data analysis. Decision making comes after exploring other processes such as gathering of data, to carrying out investigations, through interpretation of results to making decisions on the most effectively ways to utilise the results of our analysis. The quality of the decision we make after our automated analysis largely determines the amount of success that we will likely record in the course of our investigation.

SELF ASSESSMENT EXERCISE

What are the steps to the application of data-mining and automated data analysis?

4.0 CONCLUSION

Advancing effective security management and threat mitigation is an enormous task, which often demands adequate use of information technology and systemised information-gathering tools or techniques. As you may be aware, information is very vital to the security sector, without which security practitioners will be lackadaisical and highly incapacitated in the discharge of their duties. It is not a surprise that in many developed countries like the US and Britain, the government and security sector continues to undergo reforms, appreciating the strategic importance of information to the operations of various security agencies. Information plays a great role in hazard management, intelligence collection and analysis, threat mitigation, counter-terrorism, as well as overall security planning and management.

If the importance of information in security management cannot be over-emphasised, therefore, the use of data-mining and automated data analysis is very significant and useful to securitisation. The relevance of these tools has been evident in the way they have continued to enjoy growing acceptance among security practitioners in most developed countries of the world and elsewhere. These tools are powerful not only in security management and threat mitigation but they are used by several commercial institutions or corporations to improve their businesses. It is very essential to promote the use of the tools in our various places of work for efficiency and optimal performance through we can easily achieve the overall objectives of our organisations.

5.0 SUMMARY

In this unit, our study focused on the conceptual definition of data-mining, and we also described the meaning of automated data analysis. The third and the last area of inquiry was the list of processes that we undertake in the application of data-mining and automated data analysis.

6.0 TUTORED MARKED ASSIGNMENT

Define data-mining and automated data analysis; and

Explain the basic processes to the application of data-mining and automated data analysis.

7.0 REFERENCES AND FURTHER READING

Alemika, E. E. O. (2004). Crime Statistics and Information Management in Nigerian Justice and Security Systems. In E. E. O Alemika and I. C. Chukwuma (eds.). *Crime and Policing in Nigeria: Challenges and Options*, Lagos: Network on Police Reform in Nigeria (NOPRIN).

DeRosa, M. (2004). *Data Mining and Data Analysis for Counterterrorism*. CSIS Report. Washington D.C. Centre for Strategic and International Studies.

Mostashari, F. (2003). *Syndromic Surveillance in Practice: New York City*. Paper Presentation at CSIS Data Mining Roundtable. Washington D.C: Centre for Strategic and International Studies (CSIS). October 9.

Shettima, K. & Chukwuma, I. (2002). Crime and Human Rights in Nigeria. Paper Presented at the International Council on Human Rights Policy Review Seminar, themed Crime: Managing Public Order in Countries in Transition. New York, 21-22 October.

://databases.about.com/od/datamining/a/datamining.htm. Retrieved on 29 August, 2009.

://en.wikipedia.org/wiki/Data_mining. Retrieved on 29 August, 2009.

://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm. Retrieved on 30 August, 2009.

://www.cgisecurity.com/questions/falsenegative.shtml. Retrieved on 9 August, 2009.

://www.tech-faq.com/data-mining.shtml. Retrieved on 29 August, 2009.

://www.wisegeek.com/what-is-data-mining.htm. Retrieved on 30 August, 2009.