NATIONAL OPEN UNIVERSITY OF NIGERIA

COURSE CODE : CSS745

COURSE TITLE:
TYPES AND ANALYSIS OF SECURITY THREATS

COURSE GUIDE

CSS745
TYPES AND ANALYSIS OF SECURITY THREATS

Course Developer/Writer	Monsuru Adegboyega Kasali Non-Violence and Intercultural Communication Advocacy Initiatives, Ibadan, Nigeria
Course Editor	Adewole Akinyemi Atere, Ph.D College of Management & Social Sciences Osun State University
Course Coordinator	Adeniyi 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

CONTENTS   **PAGE**

Introduction

CSS 745: Types and Analysis of Security Threats is a 3-credit unit course. It is a compulsory course for all post-graduate diploma students in the field of Criminology and Security Studies of the University. The course is also recommended to any other post-graduate students especially those in the School of Arts and Social Sciences, who may have interest in the study and analysis of security threats and the mitigation techniques that can be adopted to prevent the occurrence of various threats or/and reduce the losses that may accompany the occurrence of any threats. The course can also be taken as an elective or required course by other post-graduate students whose main field(s) of discipline is not Criminology and Security Studies.

However, the Course shall consist of 20 units, which are divided into 4 modules, and each of these modules shall consist of 5 units whereby the study draws a link between one unit and the other. In the first 2 modules of this course, we focus on various areas of discourse that explain the subject- types of security threats while the last 2 modules illuminate on various threat mitigation measures and crime management approaches that can assist in no small measure to prevent, detect, and control all forms of security threats. On the whole, the units contained in the course deal with the meaning and types of security threats; basic human or manmade security threats, terrorism as a security threat; war as a security threat; information warfare as a security threat; analyses of geological, climatic and environmental threats; basic types of security; civil security approaches to threat mitigation; risk psychology and analysis; among others.

More interestingly, the material largely draws its case studies from security conditions and major threats experienced in Nigeria and Africa with the aim of exposing the reader or student to security challenges confronting Nigeria in particular and Africa as a whole. Having known that our study on types and analysis of security threats cannot

be complete if we fail to have the knowledge of the overall incidence of security threats and mitigation techniques in some other places or continents, we shall also cite examples from other parts of the world including America, Europe and Asia.

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

What You Will Learn in this Course

CSS 745: Types and Analysis of 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 that bother on the meaning and types of security threats as well as identifying many threat mitigation measures and crime detection and control mechanisms in reducing the adverse effects of various security threats on people or communities. 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 towards hazard mitigation and effective security management. Also, the reader or student will 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 at least to provide the student or reader with various ways through which he/she can reduce losses from any incidence on hazard or security attack, if you cannot prevent such threat or hazard from occurring. Knowing the impact that active involvement of civilians in security can have in complementing and increasing the capacity of the security personnel to carryout their duties effectively, the course also explores the strategic importance of civil security and how it can contribute to effective security management and threat mitigation. The issue of risk is germane to a discourse on security threats. This is because we take risks in our daily activities, and through risk psychology, we shall be explaining why some people take the issue of security risk so seriously while others do not take it seriously. In this analysis of risk, we examine how some individual or collective or governmental undertakings or actions can increase the possibility of risk, which may have either positive or adverse effects on our security or wellbeing. The material also focuses on other crime control and threat mitigation approaches including vulnerability and Capacity Assessment (VAC), Crime analysis as well as data mining and automated data analysis.

Course Aims

The overall aim of CSS 745: Types and Analysis of Security Threats as a course is to explore the meaning and types of security threats. It aims to classify various types of threats according to their peculiar conditions and features. Basically, threats are often classified as natural and human forms of security threats but this course further delineates the classification of threats into geological, climatic, environmental and human or manmade security threats for conceptual clarity and better appreciation of the subject-types of security threats. The course also explains different approaches and techniques through which security threats can be mitigated or controlled. The material describes the meaning of various types of basic security and their different approaches to general security management. These include measures to safeguard the security of computer and information systems, physical structures, infrastructure, public health, food supply among others. The course also shows the importance of civil security approaches, risk psychology and analysis, simulation, crime analysis and data mining and automated data analysis to threat mitigation and crime control. The material draws its case studies from the local and international environments. The course aims to:

- ❖ Conceptualise the term security threat;
- ❖ Identify various security threats;
- ❖ Classify or categorise various security threats;
- ❖ Discuss the meaning and types of various human or man-made security threats;
- ❖ Examine various manmade security threats;
- ❖ Explain the meaning and types of geological security threats;
- ❖ Examine climatic security threats;
- ❖ Analyse environmental threats;
- ❖ Explore how the various types of security threats pose a danger to any people or community;
- ❖ Propose measures and approaches that aid in mitigating or reducing the occurrence of different security threats;
- ❖ Unravel the importance of civil security approaches to threat mitigation and crime control;
- ❖ Elaborate the relevance of the study of risk psychology and analysis in threat mitigation and crime reduction;
- ❖ Illuminate on how simulation exercise can contribute to threat reduction and law enforcement;
- ❖ Investigate the significance of crime analyse in threat mitigation and crime management; and
- ❖ Verify how data mining and automated data analyses can serve as important tools to crime detection, control and threat mitigation.

Course Objectives

With utmost desire to achieve the aims set out above, the course has some set of objectives as demonstrated in all the units of the course. Each unit has its own objectives. Objectives are always included at the beginning of every unit to assist the student in the appreciation of what he or she will come across in the study of each unit to facilitate his or her better understanding of the course-CSS 745: Types and

Analyses of Security Threat.   The Student is, therefore, advised to read these objectives before studying the entire unit(s). The reason is that 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.

Working through this Course

In completing this course, the student is required to study the whole units, and try to read all (or 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-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- CONCEPTUAL DEFINITION OF SECURITY THREATS AND
              TYPES OF SECURITY THREATS (MANMADE)

Unit 1:   Meaning & Types of Security Threat
Unit 2:   Basic Human or Manmade Threats
Unit 3:   Terrorism as a Security Threat and Individual Protective Measures
Unit 4:   War as a Security Threat
Unit 5:   Information Warfare as a Security Threat

Module 2- ANALYSIS OF NON-HUMAN SECURITY THREATS

Unit 1:   Analysis of Geological Security Threat/Hazards I
Unit 2:   Analysis of Geological Security Threat/Hazards II
Unit 3:   Analysis of Climatic Security Threat/Hazards
Unit 4:   Analysis of Environmental Security Threat/Hazards I
Unit 5:   Analysis of Environmental Security Threat/Hazards II

Module 3- TYPES OF SECURITY AND APPROACHES TO THREAT MITIGATION

Unit 1:   Basic Types of Security I
Unit 2:   Basic Types of Security II
Unit 3:   Basic Types of Security III
Unit 4:   Civil Security Approaches to Threat Mitigation I
Unit 5:   Civil Security Approaches to Threat Mitigation II

Module 4- MEASURES FOR THREAT MANAGEMENT

Unit 1:   Risk: Meaning, Psychology & Analysis
Unit 2:   Vulnerability and Capacity Assessment
Unit 3:   Simulation in Law Enforcement
Unit 4:   Crime Analysis: Meaning and Importance to Crime Mitigation
Unit 5:   Applying Data Mining & Automated Data Analysis for Crime Management

The first module consists of five units, which will expose the student or reader to the conceptual definition of security threats and various types of security threats Within the same module, we shall be exploring and explaining different types of human or manmade security threats including robbery, theft, assassination, hijacking, terrorism, war among others. In the second module, we shall be focusing on natural threats including geological and climatic forms of threats as well as environmental threats that are often caused more by anthropogenic factors than nature. In the third and fourth modules, we shall be explaining various measures and approaches that can help in the mitigation of security threats as well as detection and control of various crimes that can pose security risk to any people or communities.

Text-Books and References

The following textbooks are recommended to students taking the course.

Berkowitz, B. J., Frost, M., Hajic, E. J. & Redisch, H. (1972). *Superviolence: The Civil Threat of Mass Destruction Weapons*. Report A72-034-10, 29 September. ADCON (Advanced Concepts Research) Corporation, Santa Barbara, CA.

Boba, R. (2005). *Crime Analysis and Crime Mapping*. Thousand Oaks, CA: Sage Publications.

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.

Jenkins, B. M. (1975). *High Technology Terrorism and Surrogate War: The Impact of New Technology on Level Violence*, (The RAND Paper Series, No. 5339) January.

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.
Wold, G.H. & Shriver, R.F. (1997). Risk Analysis Techniques. *Disaster Recovery Journal*. Available on ://www.drj.com/new2dr/w3_030.htm. Retrieved on 28 August, 2009.
International Federation of Red Cross and Red Crescent Societies (IFRC). (2006). *An Introduction to Vulnerability and Capacity Assessment*. Geneva.
Molander, R. C., Riddile, A. S. & Wilson, P. (1996). *Strategic Information Warfare: A New Face of War*. Santa Monica, California: RAND, MR-661-OSD.

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.
Dory, A.J. (2003). *Civil Security: Americans and the Challenges of Homeland Security*. Washington DC: Centre 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 the course. First are the tutor-marked assignments; secondly, 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 also 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 you are unable to complete your work on time, contact your tutor or better-still your study centre manager (overseer) before the submission deadline of assignments lapses to discuss the possibility of an extension.

Final Examination and Grading

The final examination of CSS 745 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 it takes to complete them, and the assignments that follow them.

Unit	Title	Week's Activity	Assessment (end of Unit)
	Course Guide	1	
1	Meaning & Types of Security Threat	1	Assignment 1
2	Basic Human or Manmade Threats	2	Assignment 2
3	Terrorism as a Security Threat and Individual Protective Measures	2	Assignment 3
4	War as a Security Threat	3	Assignment 4
5	Information Warfare as a Security Threat	4	Assignment 5
6	Analysis of Geological Security Threat/Hazards I	5	Assignment 6
7	Analysis of Geological Security Threat/Hazards II	6	Assignment 7
8	Analysis of Climatic Security Threat/Hazards	6	Assignment 8
9	Analysis of Environmental Security Threat/Hazards I	7	Assignment 9
10	Analysis of Environmental Security Threat/Hazards II	7	Assignment 10
11	Basic Types of Security I	8	Assignment 11
12	Basic Types of Security II	9	Assignment 12
13	Basic Types of Security III	10	Assignment 13
14	Civil Security Approaches to Threat Mitigation I	11	Assignment 14
15	Civil Security Approaches to Threat Mitigation II	11	Assignment 15
16	Risk: Meaning, Psychology & Analysis	12	Assignment 16
17	Vulnerability and Capacity Assessment	13	Assignment 17
18	Simulation in Law Enforcement	14	Assignment 18
19	Crime Analysis: Meaning and Importance to Crime Mitigation	15	Assignment 19
20	Applying Data Mining & Automated Data Analysis for Crime Management	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 attendance at 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 suits you best. Think of it as reading the lecture instead of listening to a lecturer. In the same way that a lecturer might set you some reading 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 be able to 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 chose 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 that students fail is that they get behind with their course work. If you get into difficulties with your schedule, please let your tutor know before it is too late for 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 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 unit) and the course objectives (listed in this Course Guide).

Facilitators/Tutors and Tutorials

There are between eight 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. Thus, it is the only opportunity you have to enjoy face to face contact with your tutor and to 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 in discussion activity.

Summary

CSS 745: Types and Analysis of Security Threats aims to expose the reader or student to the meaning and types and categories of security threats as well as how to explain different approaches and techniques through which threats can be mitigated or controlled. As you complete this course, you should be able to answer the following questions:

- ❖ Conceptualise the term security threat;
- ❖ Identify various security threats;
- ❖ Classify or categorise various security threats;
- ❖ Discuss the meaning and types of various human or man-made security threats;
- ❖ Examine various manmade security threats;
- ❖ Explain the meaning and types of geological security threats;
- ❖ Examine climatic security threats;
- ❖ Analyse environmental threats;
- ❖ Explore how the various types of security threats pose a danger to any people or community;
- ❖ Propose measures and approaches that aid in mitigating or reducing the occurrence of different security threats;
- ❖ Unravel the importance of civil security approaches to threat mitigation and crime control;
- ❖ Elaborate the relevance of the study of risk psychology and analysis in threat mitigation and crime reduction;
- ❖ Illuminate on how simulation exercise can contribute to threat reduction and law enforcement;
- ❖ Investigate the significance of crime analyse in threat mitigation and crime management; and
- ❖ Verify how data mining and automated data analyses can serve important tools to crime detection, control and threat mitigation.

Good luck in your studies at the National Open University of Nigeria.

CSS745   TYPES AND ANALYSIS OF SECURITY THREATS

Course Developer/Writer	Monsuru Adegboyega Kasali Non-Violence and Intercultural Communication Advocacy Initiatives, Ibadan, Nigeria
Course Editor	Adewole Akinyemi Atere, Ph.D College of Management & Social Sciences Osun State University
Course Coordinator	Adeniyi 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

CONTENT   **PAGE**

MODULE 1: CONCEPTUAL DEFINITION OF SECURITY THREATS AND TYPES OF SECURITY THREATS (MANMADE)

UNIT 1

MEANING & TYPES OF SECURITY THREATS

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Body
    3.1   Meaning of Security Threat
    3.2   Types of Security Threats
        3.2.1 Geological Threat/Hazards
        3.2.2 Climatic Threats/Hazards
        3.3.3 Environmental Hazard
        3.3.4 Human Threats
4.0   Conclusion
5.0   Summary
6.0   Tutor Marked Assignment
7.0   References / Further Reading

1.0.   INTRODUCTION

The meaning of security has been generating a great debate among scholars in recent time. The experience of the world in recent time emphasises a paradigm shift in security discourse. Traditionally, the State is the custodian and ultimate beneficiary of the monopoly use of violence as advocated by Max Weber. Any internal or external threat to 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 all over the world. 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.

However, this is evident in the enormous political sovereignty enjoyed by international terrorist networks, which have created their own governments, standing armies 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 recent experience shows 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 draws our attention to the amount of threat that poverty and deprivation can pose to security in any community or state. In this unit, we shall define the term security threat and briefly explain various types of threat.

2.0   OBJECTIVES

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

- Explain the meaning of security threat;

- Identify types of threat; and

- Explain forms of natural and human threats.

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:

...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 capacity of any human and non-human elements to destroy the vital interests of other considered as targets. We can also describe security threat as:

...*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).

...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 be simply 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.

SELF ASSESSMENT EXERCISE

How do you describe the term security threat?

3.2   Types of Security Threats

As explained earlier, security threats can be classified into two namely natural and manmade threats. Natural threats can further be divided into two: minor and major. Examples of major natural threats may include hurricane (cyclone), earthquake, drought and flood. And those natural threats or hazards considered to be minor may include cold wave, storm, mudslide, thunderstorms, to mention a few. In this study for the sake of conceptual and analytic clarity, we shall be explaining the natural threats by dividing them into two due to different conditions, and they shall be classified as geological security threats and climatic security threats.

On the other hand, manmade threats usually involve those threats or hazards that are brought into bear resulting from human actions (deliberately or accidentally). These threats may include terrorism, different forms of crime, mob action, kidnapping, among others. The third type of security threat may include all forms of environmental threat or hazard. At this point, let us present these various types of security threats one after the other.

3.2.1 Geological Threat/Hazards

Geological threats or hazards are basically natural geologic phenomena, which can potentially pose a huge security risk to human lives, as they are not only capable of causing various degrees of bodily harms to people but can also cause (mass) deaths. They can also bring on any communities or people large-scale destruction of physical structures and infrastructure. Thus, geological threats or hazards can be simply defined as:

...extreme natural events in the crust of the earth that pose a threat to life and property, for example, earthquakes, volcanic eruptions, tsunamis (tidal waves) and landslides (://stats.oecd.org/glossary/detail.asp?ID=1112).

As highlighted in the foregoing, the hazardous processes any communities that can pose a danger to people and their environments may include earthquakes, volcanic eruptions, flooding, mudflows, tsunamis to mention a few. It is also important to note that the set of threats cannot be easily detected as they largely remain unpredictable.

Though, through hazard mapping and monitoring, we can determine the locations or areas that are susceptible to the various kinds of natural threats that exist in this class of threats but, we may not have accurate prediction of the time that these hazards may occur in any place. For this reason, it is usually advisable to identify the kinds of natural hazards that may exist in our communities. For instance, those areas or settlements that lie along the seismic lines, there is possibility that they will experience earthquake at one time or the other. It is paramount for the people found in such locations to erect their physical structures in a way that they will be resistant to the vibration that is usually produced by the quake.

3.2.2 Climatic Threats/Hazards

Climatic threats or Hazards are simply those types of threat that involve a rapid change in the climatic conditions, capable of posing a danger to the wellbeing and survival of any people or communities. They are natural threats that are usually created by:

...a severe variation from average climatic conditions which cause problems for the people living in the area affected (://www.geography-help.co.uk/powerpoints/human_activities_ctwm_monsoon.ppt).

Climatic hazards are actually created by one or a combination of factors which may include heavy rainfall, droughts, wildfires, among others. Climatic hazards basically include hurricane, flood and drought. It is important to avoid mistaking climatic problem for climate hazard. For instance, drought can be regarded as a climatic hazard where there is usually regular experience of rainfall because rapid reduction in the volume of rainfall in such a settlement or place can be considered as hazardous. And in desert area or arid settlement, the incidence of drought is usually viewed as climatic problem rather than hazard because people found in such an area or settlement are used to dry weather with very little prospect for rainfall.

Meanwhile, human activities such as deforestation among other anthropogenic factors can also contribute to the occurrence of these climatic hazards. For instance, continued emission of greenhouse gases notably carbon dioxide into the atmosphere has been a leading factor to the problem of climate change with devastating consequences on man and his/her environment.

3.3.3 Environmental Hazard

Environmental Hazards are types of threat, which usually involve entrapment of the environment with various forms of pollution like bush burning, reckless removal of trees, use of chemicals among others. There is no doubt that environmental hazards constitute a huge security risk to any people or community. These hazards can generate such devastating situations as air pollution, water pollution as well as soil contamination.

Anthropogenic factors are chiefly responsible for various environmental pollutions that generate different environmental hazards. The consequences of these hazards can be very severe and unpleasant to any people because apart from the adverse effects that it may have on people's health and wellbeing, it can also bring the economy of affected communities to its knees, creating an atmosphere of economic underdevelopment.

3.3.4 Human Threats

Human threats are basically any intentional criminal actions like terrorism, kidnapping robbery, theft, etc. They also include any other unintentional actions that may pose security risk to any people or communities such as careless handling of information files, among others.   When we talk about information technology (IT) one of the issues that come to our minds is the growing risk emanating from the activities of hackers and other people that engage in malicious entry into information systems. In view of this, several human activities can pose a threat not only to the wellbeing of the people but can also propel physical, infrastructural and information damages or destructions.

Undoubtedly, the activities of disloyal employees can rapidly effect the collapse of any corporations if adequate mitigation measures are not put in place to check the mischief of such workers. Apart from the normal criminal actions, human beings have also been accused of being responsible for the invocation of most of the natural threats. For instance, variability in climate conditions is normal but human emission of greenhouse gases into the atmosphere has rapidly led to drastic and significant change in the world climate, putting biodiversity into quandary.

The challenges confronting mankind resulting from climate change are enormous leading to growing reduction in the volume of rainfall and resource scarcity, to mention a few. There are some other forms of security threat that we may not be covering in this course. It is, therefore, important to engage in further reading to identify other types of threat not discussed in the material.

SELF ASSESSMENT EXERCISE

Discuss various types of 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 necessary 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.

5.0   SUMMARY

In this unit, we began our journey into the course (Types and Analysis of Security Threats) by examining the meaning of security threats. Thereafter, our focus was shifted to various classes of security threats such as geological threats/hazards, climatic threats/hazards, environmental threats as well as human or manmade threats. We also observed that there are other classes of security threats that we may not able to cover in this material, as the reader or student is admonished to source for other relevant materials that can help them identify some other types of threat not discussed in this course. In the next four units, we shall be beaming our searchlight on some of the threats that can be considered as manmade while other classes of security threats will be discussed in the next module.

6.0   TUTOR-MARKED ASSIGNMENT

Explain the meaning and any four types of security threats.

7.0   REFERENCES AND FURTHER READING

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.

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.

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

://stats.oecd.org/glossary/detail.asp?ID=1112. Retrieved on 14 November, 2009.

://www.geography-help.co.uk/powerpoints/human_activities_ctwm_monsoon.ppt. Retrieved on 20 November, 2009.

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

UNIT 2

BASIC HUMAN OR MANMADE SECURITY THREATS

CONTENTS

1.0   Introduction

1.0.   INTRODUCTION

In the last unit, our study centred on the meaning of security threat, and we also explained various forms of threats including geological threats, climatic threats, environmental threats and human or man-made threats. In furtherance of our study on these different classes of threats, we shall beam our search light on various types of threats contained in each class of security threats by exploring their meaning and how they can constitute a danger to any people or communities. In this unit, we shall be focusing on human or man-made threats by exploring some of the basic types of man-made threats and showing how they can pose security risk.

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

3.0   MAIN BODY

3.1   Robbery

One of the 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 any other dangerous objects as the case may be, are often used by robbers to force the victims to yield to their (robbers') demand. There are many definitions of robbery, some of which include the following:

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 the crime of seizing property through violence or intimidation (://en.wikipedia.org/wiki/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 jewellery 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).

Robbery is a regular feature of every human society, even among the animals, robbery takes place. For instance, in some wildlife clips, we may see some hyenas hunting some preys and eventually they may succeed in catching some of these preys like antelopes. But, shortly after the catch, we may see a group of lions larger in number emerging 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 it also exists in animal kingdom.

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 which 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 time. 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 some passengers against some other passengers on the same vessel. The phenomenon of piracy is 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) <u>Car-snatching or Carjacking</u>: 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 through 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 (<u>://ww.knowledgerush.com/kr/encyclopedia/Carjacking</u>).

In some situations, the car-snatcher may use toy gun to force the victim (carry owner or driver) out of 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 children. Can you imagine the amount of trauma suffered by the children, seeing their father and breadwinner 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 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 whereby cars will be 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 not car-snatching or carjacking;

c) Streaming: This is another of robbery that usually involves organised criminal activities being perpetrated on underground trains. The term is made popular by the United Kingdom, used to describe the violent crimes perpetrated on train or bus passengers by criminal gangs (see   ://news.bbc.co.uk/1/hi/england/698 3476.stm; & ://www.btp.presscentre.com/Content/Detail.asp?Release ID=6 75&NewsAreaID=2). 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 be simply 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 on-coming trailer, which was on top speed while trying to avoid being pinned-down by the robbers. The ugly incident happened when the victim passengers were asked by the robbers to lie 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. In armed robbery, the weapons used by robbers may not be actually deadly. 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 do not 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 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, organisation(s) also can be found culpable. For instance, several organisations have been accused of stealing information belonging to some other organisations, may be through the use of an insider or through 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 the recharge card. In the situation whereby the person in question decides to sell or use the recharge card,

he/she has committed theft, showing 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 this happens, the act can no longer be regarded as theft but it 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 criminal intention of illegally getting claims from an insurance company. Meanwhile, most times this crime is perpetrated by a party against another party. The antagonistic and destructive activities that dominate our national politics has paved the way for the growing anarchy that the country experience.

From one democratic dispensation to another, the incidence of arson has featured not only in inter-party relations but also in intra-party wranglings. The use of thugs to set fire on the houses of opponents is still experienced in Nigerian politics. For instance, in the last re-run governorship election in Ekiti State of Nigeria saw the burning down of the Independent National Electoral Commission's (INEC) office in Ido Ekiti by irate youths over the alleged manipulation of election results by the election body and 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 financial and 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 their noses 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 of the definition of the term kidnapping. 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 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)](://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 south-eastern Nigeria where the business of kidnapping is becoming widely accepted among the youth 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 has been a major source of worry to the security sector, especially as security personnel are not left out by kidnappers. For instance, some practitioners have 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. The risk created by this threat is to deepen the vulnerability of the affected individuals by setting him/her up. Here, the individual like a security officer is coerced to compromise his position by tricking him/her into a social action or activity that people will not expect persons in such position to engage in. For instance, a very principled security chief may be trapped with a woman, and his conversations and sexual relations with the woman are recorded by his enemies who set him up in the first instance.

Consequently, the enemies will approach him and ask him to compromise his position or he will be blackmailed. This scenario reemphasises the need for security practitioners to always be very careful in their relation with other people and avoid engaging in any action that can tarnish their image and that of the offices 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 certain money or property or services to the offender. On daily basis, 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 offence, 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. The 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. And one of the consequences of this failure is circulation of proliferated weapons in the country, which came 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 company of a friend, being intercepted by an anti-robbery patrol team before 8pm when there was no case of curfew, and subsequently 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 through 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. Unfortunately, the experience of most civilians, resulting from official and unofficial extortion by security operatives in the country undermines the integrity and capacity of the public security sector in fulfilling 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/68 079).

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 an 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 the 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 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   **Strike Action**

Strike action is often described as refusal of employees to report at their workplaces or/and refusal to discharge their respective duties in protest against poor working conditions and/or policies of authorities or government or employers which they consider inimical to their welfare and wellbeing. Since the period of industrial revolution, strike action has become a veritable tool used (as the last resort) by different unions to express their grievances and prevail on the authorities or employers to yield to the labour demands.

Undoubtedly, strike action can potentially constitute a threat to any regime, as it can lead to the loss of huge amount of working hours and money. For instance, the strike embarked upon by labour unions in the early 1990s in reaction to the annulment of the June 12, 1993 presidential election by General Babangida almost degenerated to total collapse of socio-economic activities in Nigeria. The strike also had a devastating effect on the political administration of the Nigerian state, as the military government under Late General Sani Abacha resorted to carrying out unlawful arrests on the union leaders and several human rights activists to legitimise his unconstitutional rule after taking over from Chief Ernest Shonekan, the leader of the interim government put in place by General Ibrahim Babangida when he failed in his transition programme before he relinquished his position as military leader of Nigeria.

Types of Strike

Wildcats Strikes: These are a form of strike or industrial show-down whereby workers or employees embark on work boycott without being mandated by their respective (labour) unions. They may decide to embark on such strikes if they consider that the

leaderships of their unions are not actually supporting their intention to force their employers to yield to their demands through industrial action or if they suspect that their unions have betrayed them. Wildcats strikes are often regarded as unofficial strikes because they are embarked upon by employees without any formal authorisation from the unions. They are capable of posing huge security risk to any organisation or government as the employers may find it difficult to negotiate with the striking workers because of the distance that might have been created between the employees and their union leaderships. Thus, decisions made with the union may not be accepted by the striking workers with little opportunity for collective bargaining.

Sit-Down Strike: This is another type of strike, which usually involves workers' presence at their places of work but they will not perform any official duties. Here, striking employees will only boycott their duties but not places of work.

Work-to-Rule Strike: This form of strike is known in Italy as *Sciopero bianco*. In this strike, workers report for duties and perform their various tasks but they will fail to improve on their inputs in production processes by following very strictly all safety regulations. For instance, striking police personnel may report to their respective duties but through this form of strike, they will not respond to any emergency calls in the absence of operational equipment like patrol vehicles, as well as non-availability of bullet proof vests.

Meanwhile, we may have observed that even without operational vehicles, police patrol teams still manage to use commercial vehicles to perform their duties. But, due to work-to-rule strike, they will insist that they will not do the patrol or emergency intervention if there are no official vehicles. In this case, there is tendency that the services that will be rendered by the police will be insufficient in the management of security of lives and property in any community especially where there is no adequate funding of the police like Nigeria.

General Strikes: These are usual strikes which involve employees acting on the directives of their unions to embark on work boycott in their reaction to poor working conditions and as last resort to compel the authorities or employers to yield to their demands. General strikes also pose huge security threat to any nation or organisation owing to the amount of time and money wasted resulting from the industrial action. For instance, in Nigeria, no less than five hundred billion Naira must have been lost in the last three years as a result of regular face-off between Labour Unions and Government at all levels, leading to a series of strikes.

Sympathy Strike: It is another form of strike that is undertaken by the workers of a union supporting the workers of another union who are on strike by refusing "to cross a picket line established by another as a means of supporting the striking workers" (://en.wikipedia.org/wiki/Strike_action).

Student Strike: This form of strike has impact on public image of any country rather than its economy. Here, the students embark on boycott of lectures and other academic activities to express their displeasure towards some of the policies of the

authorities or government. This strike action by the students is often supported by the teachers especially if the aim of the strike is to press the authorities or government to improve the working conditions of their teachers. Student strike can also pose a risk to the community because such action is often followed with demonstration that may become bloody if not maturely handled by security personnel and school authorities.

Hunger Strike: This is another form of strike, which poses very little or no threat to any community other than the negative impact that such action may have on the image of the community. It actually involves intentional refusal to eat to protest against some actions of government or authorities.

Sick-out Strike: This type of strike is also known as "blue flu" strike, and it usually involves the striking workers pretending as if they are sick as a way of refusing to work. As you may know, there are some employees whose nature of their professions does not permit them to go on strike. In many countries including Nigeria, police, military, fire-fighters as well as air controllers are constitutionally barred from embarking on strike because such action is mostly likely to generate breakdown of law and order as well as collapse of public safety.

SELF ASSESSMENT EXERCISE

Explain the meaning and types of strike action.

3.9   **Assassination**

Assassination is another form of manmade security threat. Etymologically, the word Assassin emanated from the Arabic word *Hashshashin*. The term usually involves a target killing of any political leader or any other person for ideological or political or military or even economic reasons. Traditionally, assassination was synonymous to (covert) government-sanctioned killing of any people especially the opponents for political reasons (see ://www.washingtontimes.com/news/2004/mar/25/20040325-091452-7923r).

The use of assassination by leaders has long been supported by some political philosophers and military strategists. For instance, Sun Tzu in his book, The Art of War lent his weight behind the use of the strategy of assassination for military purposes while another great writer, Nicollo Machiavelli contended in his book, "The Prince" that assassination could be a very tactical instrument for political rulers to retain and consolidate their grips on political power and preserve their regimes.

Assassination can also constitute a huge security threat to communities or people. The use of assassination by any individuals or authorities can potentially undermine the capacity of law enforcement agents in managing local and international security. For instance, the spate of political assassinations that has greeted Nigeria in the last eight years has nevertheless made rubbish of the ability of the Nigeria Police to guarantee the security of lives and property of the citizens. The situation has really had a

devastating effect on the economic wellbeing of Nigerian state owing to the demonising image that the ugly trend of political assassinations have brought on Nigerian people. Many well-meaning Nigerians who can contribute greatly to national growth are not willing to vie for elective positions for the fear that they may be killed or assassinated by opponents, further complicating the problem of the nation's underdevelopment.

SELF ASSESSMENT EXERCISE

What is assassination, and how does it pose a security threat?

3.10 **Demonstration**

Demonstration is another manmade threat that also has the tendency to pose a danger to any community. Demonstration may also be regarded as civil disturbance or direct action. It is often undertaken for different reasons but most times, demonstration is politically motivated. For instance, during the military rule of General Abacha, many human-rights and pro-democracy activists as well as several other individuals including students staged demonstration to protest the continued detention of Chief Moshood Abiola and continued sojourn of the military in governance.

There are two basic type of demonstration, and they are violent and non-violent demonstrations. Violent demonstrations largely constitute huge security risk, as it can lead to the breakdown of law and order. Violent demonstration may generate wanton destruction of lives and property. On the other hand, non-violent demonstration normally involves the use of peaceful approaches like strike, the use of graffiti etc.

SELF ASSESSMENT EXERCISE

Explain demonstration as a security threat.

3.11 **Mob Action**

Mob Action is a potential form of manmade threat. It is usually a crowd or large gathering of people with strong emotional convictions that often lead them to act in violent or criminal or unlawful ways. Many people have been killed through mob actions. For instance, the bloody rivalry between United Party of Nigeria (UPN) led by late Chief Obafemi Awolowo and National Party of Nigeria (NPN) led by Alhaji Shehu Shagari and Chief Adisa Akinloye resulted in a series of mob actions in South-western Nigeria where the supporters of these rival parties in groups violently attacked opponents with high record of arson and killing. There is no doubt, mob action can really undermine the security of lives and property in communities.

SELF ASSESSMENT EXERCISE

Describe mob action as a manmade threat.

4.0   CONCLUSION

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 adverse impact that manmade security threats may have on any community 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 weapons 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 organisations (NGOs) through bilateral or multilateral arrangements to discourage proliferation of weapons or the use of deadly weapons for global security.

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, among others. 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. Some of these threats include corruption and embezzlement, gender discrimination, ethnocentrism, to mention a few. You are, therefore, advised 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. In the next three units, we shall be focussing on some other types of manmade threat.

6.0   TUTOR-MARKED ASSIGNMENT

Discuss any five types of manmade security threat.

7.0   REFERENCES AND FURTHER READING

English Dictionary (1989). Second edition.

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.

://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/Strike_action. Retrieved on 10 November, 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.

://www.washingtontimes.com/news/2004/mar/25/20040325-091452-7923r. Retrieved on 3 0ctober, 2009.

UNIT 3

TERRORISM AS A SECURITY THREAT AND INDIVIDUAL PROTECTIVE MEASURES

CONTENTS

1.0   Introduction
2.0   Objectives

3.0   Main Body
    3.1   Meaning of Terrorism
    3.2   Aspects of Terrorism
        3.2.1 Chemical Terrorism
        3.2.2 Cyberterrorism
        3.2.3 Bioterrorism
        3.2.4 Radiological Terrorism
        3.2.5 Physical Violence
    3.3   Individual Protective Measures
4.0   Conclusion
5.0   Summary
6.0   Tutor-Marked Assignment
7.0   References / Further Reading

1.0   INTRODUCTION

Terrorism is not a new 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 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. Terrorism has a long history. In the 12th century, the Assassins, a terrorist network, an *Ismaili* sect of Shiite Muslims advanced some hostilities against *Sunni* Muslims. In 1408, John Wyclife, a theologian escaped death but several hundreds of his followers were not lucky as they were burnt to death. The reason was that Wyclife translated the Latin Valgate Bible into English in a way not favourable to the doctrine of trinity.

In the aftermath of reformation; there had been a terrorist combat between the catholic and protestant dissidents in Ireland; that culminated into the creation of the Irish Republican Army (IRA), which grew out of the Irish civil Rights movements in the 1960s. IRA has on several occasions attacked the British civilians. It declared a cease-fire in August 31, 1994, but resumed hostilities on 15 September 1997. In Spain, Basques separatist organization (ETA) has carried several terrorist operations in which more than 1000 Spaniards were killed, kidnapped or maimed. The long anarchist tradition and instability in the Italian political system propelled the inauguration of terrorist movements in Italy. The most notable among them was the Red Brigades whose terrorism activities reached a crescendo in the 1978 kidnapping and killing of Aido Moro, a former prime minister.

In the old West Germany, Red army faction also known as the baader- Meinhof Gang conducted series of terrorist operations both within and outside their immediate territory. They specialized also in Bank robbery. By 1970s, the activities of terrorists reached a descending order. The subject of terrorism much more became a global debate due to the September 11, 2001 terrorist attack where commercial aircrafts were

used as weapons of mass destruction by terrorists linked to the Al Qaeda network led by Osama bin Laden. In this unit, we shall discuss various important issues on the subject of terrorism as a security threat.

2.0   OBJECTIVES

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

- Describe the term terrorism;

- Discuss various forms of terrorism;

- Explain various aspects of terrorism; and

- Clarify a number of individual protective measures towards mitigation of terrorism.

3.0   MAIN BODY

3.1   Meaning of Terrorism

Conceptually, Wilkinson (1977) observes the underlying problem or dilemma which detonates the subjective nature of terror. The "complex interplay of the subjective forces and …frequently irrational individual responses" (Wardlaw, 1989: 8) make the definition of terrorism a utopian project (Wilkinson, 1977). It is often said that the use of terror is not always characteristic of terrorism such that:

...the killing of one soldier on field of battle by another is not 'terrorism'; the threat by one state that it will assist another if that is attacked is not 'terrorism', the shooting of a person in a store during a robbery is not 'terrorism'. It is apparent that while these acts can constitute terrorism, the definitional answer depends on other factors too (Higgins, 1997: 15).

Then, what constitutes terrorism? The definitional problem of terrorism begs for more questions than answers. Is slave trade an act of terrorism? Does a state territorial aggression or occupation of another state constitute terrorism? Does imperial conquest constitute terrorism? Does violence generated through ethnic nationalism and struggle for self-determination constitute terrorism? Does the violence emanating from the advancement of religious fundamentalism constitute terrorism? Is application of terror to combat terror, an act of terrorism? These questions may lead us to the question of morality and justification of violence. However, pacifists contend that the use of terror as a means to an end or as an end in itself is obsolete, immoral and absurd because 'there can be no morally valid authorization to kill human beings' (Claude, 1983: 4). On the definition of terrorism, According to Hardman, terrorism can be defined as;

...the method or the theory behind the method whereby an organized group or party seeks to achieve its avowed aims chiefly through the systematic use of violence (Hardman, 1937).

...extraordinary violence. It is intended to create massive fear and involves a planned attack for a purpose, often against something or someone. Terrorism is meant to have an audience. The differences between various terrorist attacks involve the people, purpose, and how it is carried out ([://edhelper.com/Reading Comprehension_33_243.html](://edhelper.com/ReadingComprehension_33_243.html)).

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, the 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).

SELF ASSESSMENT EXERCISE

Explain the meaning and forms of terrorism

3.2   Aspects of Terrorism

There are several aspects of terrorism, which range from conventional ones to non-conventional aspects. In this segment of the unit, we shall be explaining the numerous aspects of terrorism to stimulate our better appreciation of the subject (terrorism). It is important to know that we cannot cover every aspect of terrorism in this study due to the dynamics of terrorism as a security threat, compelling further inquiries into its meaning, effects, operations, among other areas of discourse by scholars. For instance, before September 11, 2001, terrorist attacks against the United States, no one could have thought that commercial planes could be used by terrorists as weapons of mass destruction as it became evident in that ugly phenomenon.

3.2.1 Chemical Terrorism

Chemical Terrorism is one of the aspects of terrorism. It involves the application of chemical agents like poisonous gases, liquid or solid that may have very toxic effects on any targeted persons and ecosystem. It can also be defined as "the use of a chemical agent in a terrorist incident and to intentionally inflict harm upon others (.nmmems.org/main_glossary_C.html).

The destructive nature of these chemicals can potentially result in serious injuries or deaths of the victims and even the terrorist offender. The amount of fatality that may accompany this form of terrorism depends largely on the type of chemical agents used by the terrorists and the duration of the exposure. However, according to the United States Centre for Disease Control and Prevention (CDC), these chemical agents can be classified as:

- **Blistering (Vesicant) Chemicals**
    - Distilled Mustard (HD)
    - Lewisite (L)
    - Mustard Gas (H)
    - Nitrogen Mustard (HN-2)
    - Phosgene Oxime (CX)
    - Ethyldichloroarsine (ED)
    - Lewisite 1 (L-1)
    - Lewisite 1 (L-2)

- o Lewisite 1 (L-3)
- o Methyldichloroarsine (MD)
- o Mustard/Lewisite (HL)
- o Mustard/T
- o Nitrogen Mustard (HN-1)
- o Nitrogen Mustard (HN-3)
- o Phenodichloroarsine (PD)
- o Sesqui Mustard
- **Blood Chemicals (chemicals acting on the blood)**
  - o Arsine (SA)
  - o Cyanogen Chloride (CK)
  - o Hydrogen Chloride
  - o Hydrogen Cyanide (AC)
- **Choking/Lung/Pulmonary Damaging Chemicals**
  - o Chlorine (CL)
  - o Diphosgene (DP)
  - o Nitrogen Oxide (NO)
  - o Perflurorisobutylene (PHIB)
  - o Phosgene (CG)
  - o Red Phosphorous (RP)
  - o Sulfur Trioxide-Chlorosulfonic Acid (FS)
  - o Teflon and Perflurorisobutylene (PHIB)
  - o Titanium Tetrachloride (FM)
  - o Zinc Oxide (HC)
- **Incapacitating Chemicals**
  - o Agent 15
  - o BZ
  - o Canniboids
  - o Fentanyls
  - o LSD
  - o Phenothiazines
- **Nerve Chemicals**
  - o Cyclohexyl Sarin (GF)
  - o GE
  - o Sarin (GB)
  - o Soman (GD)
  - o Tabun (GA)
  - o VE
  - o VG
  - o V-Gas
  - o VM
  - o VX
- **Riot Control/Tear Chemicals**
  - o Bromobenzylcyanide (CA)
  - o Chloroacetophenone (CN)
  - o Chloropicrin (PS)

- o CNB - (CN in Benzene and Carbon Tetrachloride)
- o CNC - (CN in Chloroform)
- o CNS - (CN and Chloropicrin in Chloroform)
- o CR
- o CS
- **Vomiting (Emetic) Chemicals**
  - o Adamsite (DM)
  - o Diphenylchloroarsine (DA)
  - o Diphenylcyanoarsine (DC)
- Other Industrial Chemicals (://www.medterms.com/script/main/art.asp?articlekey=18694).

3.2.2 Cyberterrorism

Since the 1990s, computer technology has begun to attract wide acceptance and popularity among the world population irrespective of age brackets, occupation, class, education and gender. Computer appreciation has become an issue of interest not only as a mechanism for information but also a subject of development. The knowledge of Computer has become universalised such that one's literacy is also determined by his/her ability to use computer and capacity to learn and share knowledge electronically.

It is not surprising that most corporations and business outfits are using computers as platforms to showcase their products to consumers and engage in all sorts of transactions. Nevertheless, the issue of cyberterrorism has attracted growing global concern because of the very destructive impact that it has not only on world polity but also its capacity to undermine economy and development of any nation. Conceptually, how do you define the term, cyberterrorism? It can simply be defined as:

...the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication (://www.dawn.com/weekly/dmag/archive/020616/dmag21.htm).

As computers are used to perform variety of legitimate function, some individuals and organisations explore the use of computer to perpetrate different criminal activities like malicious system intrusion, virus attacks, etc. The phenomenon of cyberterrorism has become more visible in recent time especially due to very destructive use of information technology to cause data damage by some disgruntled or fraudulent elements.

3.2.3 Bioterrorism

Biological terrorism or simply put, bioterrorism is another aspect of terrorism that can have very devastating effects on any people. What is bioterrorism? According to the US Centres for Disease Control and Prevention (CDC), bioterrorism can be defined as:

...the deliberate release of viruses, bacteria, or other germs (agents) used to cause illness or death in people, animals, or plants. These agents are typically found in nature, but it is possible that they could be changed to increase their ability to cause disease, make them resistant to current medicines, or to increase their ability to be spread into the environment (quoted on ://www.hhs.gov/disasters/emergency/ manmadedisasters/bioterorism/index.html).

Bioterrorism can also be described as:

...intentional release or dissemination of biological agents (bacteria, viruses, or toxins); these may be in a naturally-occurring or in a human-modified form (://en.wikipedia.org/wiki/Bioterrorism).

...the employment of living agents such as viruses, bacteria, and other biological toxins to attack or intimidate societies or governments, often for political or ideological reasons (www.pbs.org/wgbh/rxforsurvival/glossary.html)

Bioterrorism may range from contamination of products with the use of some harmful biological agents to application of aerosolised anthrax and even a number of very virulent biological agents like Type-A botulinal toxin, capable of decimating the population of any target people or community. For instance, a small quantity of botulinal toxin (BTX) can potentially kill millions of people within a short period of time (see Jenkins and Rubins, 1978: 224). The high level of toxicity of biological agents was captioned by Berkowitz *et al*. (1972):

The potency of the pathogens on a weight basis exceeds that of the most toxic chemicals; between a few and a few thousand viable organisms is all that is required to produce infection in many cases. Since pathogens can be prepared in concentrations of the order of 10^{10} microorganisms per gram, infectious doses range downward from 0.1 microgram per target individual. The search capability of the aerosol cloud and the fact that infectious doses are independent of victim bodyweight (because the pathogen reproduces in the host), make the quantity of BW material needed for mass attack quite small indeed (Berkowitz *et al*., 1972: VIII-54).

Bioterrorism poses a huge threat to the security of lives of any people because of its very virulent and destructive nature. The use of biological agents has the capacity to cause mass deaths in any target community. It is worrisome that small quantities of these destructive biological agents are only needed by terrorists to bring situation of mass destruction and murder on any target people or community due to their titanic lethality. These agents can be produced anywhere and cannot be detected easily, and above-all, it is cheap to acquire compared to nuclear weapons.

If the argument made by a number of sources that HIV-AIDS is a product of biological warfare is anything to go by, considering the high casualty level recorded by the disease, we may not but agree that bioterrorism constitutes very high security risk not only nationally but also internationally. In Africa alone, it is projected that between 90 and 100 million deaths must have been recorded by 2025 resulting from AIDS (://www.guardian.co.uk/world/2005/mar/04/aids). There are various categories of critical biological agents with varying degrees of virulence and these include:

Category A

This set of biological agents involves high-priority agents that are very destructive and can pose huge threat to any community. Apart from their high mortality, they can be dispersed without any (public notice). Thus, they cannot be easily detected and they have the capacity to bring the public health of any target community to a comatose. They include variola major (smallpox); *Bacillus anthracis* (anthrax);*Yersinia pestis* (plague); *Clostridium botulinum* toxin (botulism); *Francisella tularensis* (tularaemia); filoviruses etc.

Category B

This category of biological agents consists of those agents that can be considered of having the tendency of causing less risk to any people or communities compared to those agents contained in category A. Their level of morbidity and mortality is lower than the biological agents in category A. It is moderately easy to disperse this category of biological agents. Examples of these agents may include *Coxiella burnetti* (Q fever); *Brucella* species (brucellosis); *Burkholderia mallei* (glanders);   alphaviruses, etc.

Category C

In this category, we have those biological agents or pathogens that can be nurtured and they can also be dispersed easily but with high potential to cause high morbidity and mortality. These agents can also have very devastating effects on the public health of any target communities, and they may include Nipah virus, hanta viruses, tickborne hemorrhagic fever viruses, tickborne encephalitis viruses, yellow fever, and multidrug-resistant tuberculosis.

3.2.4 Radiological Terrorism

Radiological terrorism is another aspect of terrorism, which involves an act of dispersing radiological devices with the aim of causing public panic or attacking nuclear facilities in an attempt to undermine the security of any people or communities. There is no doubt that radiological terrorism can pose high security risk to any people. Though, its usage to attack nuclear facilities has been reportedly very

few, nevertheless there has been anxiety and palpable fear among the world population about the huge threat that such attacks may bring into bear (**Error! Hyperlink reference not valid.**). Conceptually, if terrorism can simply be defined as act(s) of causing frightening or fear especially through systematic use of violence, then how do we define radiological terrorism? Basically, radiological terrorism can be defined as:

Terrorist acts carried out either by attacking a nuclear facility or through malicious use of a radiological device (.atomicarchive.com/Glossary/Glossary8.shtml)

...the deliberate use of radioactive material to cause destruction, contamination, and injury (://www.stimson.org/pub.cfm?ID=472.).

Radioactivity can be described as the property of a number of elements that propels a impulsive conversion or decay of the nucleus of an unstable atom. Thus, as the unstable atom attempts to transform itself to a stable state, it definitely discharges energy in the form of radiation. Radioisotopes (radioactive materials) are the substances used for this process of transformation. When the substances are developed into a usable form like powder or pullets, they become radioactive sources (://www.nti.org/h_learnmore/radtutorial/chapter01_05.html).

Through the use of radiological dispersal device (RDD) containing some radioactive materials, terrorists can pose a high security risk to any people especially by causing severe physical and environmental contamination. For instance, the use of "dirty bomb", a type of RDD that involves the use of normal explosives like TNT, to violently disperse radioactive materials, can also cause serious physical and environmental damage. Apart from usual violent destructions often precipitated by the blast emanating from the bomb, the explosion will also disseminate radioactive materials to contaminate the environment, capable of putting the public health of the affected communities in quandary. These radioactive materials can cause different forms of ailment including cancer.

There are two ways through which terrorists can use radiological materials, and they include active and passive. The active approach usually involves disseminating radioactive materials over wide or small area with the application of RDD. On the other hand, passive approach normally involves spreading of radioactive materials in form of radiation-emitting device (RED) in a location with the aim of infecting the people with the harmful materials. RED can be disseminated in a busy public place where many people can be infected with the materials, causing them a lot of harm on either a long or short term depending on the destructive nature of the materials used.

3.2.5 Physical Violence

Physical violence is generally one of the aspects of terrorism. It is actually a regular feature of terrorism. It usually involves the use of aggression and physical attack that can cause harm in human and material terms to any target people or communities.

This aspect of terrorism does not always involve the application of biological or chemical or radiological agents or any highly technological weapons. Though, we cannot rule the use of any of the foregoing but it normally involves the use of small arms and light weapons like rifles, grenades, etc.

A good example is the December 1986 terrorist attack in Columbia where there was bomb explosion outside a government office building in Bogotá. In the aftermath of that dastardly act, fifty-two people were reported dead. A long bloody conflict between the Drug commandos and government forces in Columbia has been recorded. In august 1989, the Columbian government declared a war against the drug barons. Within three months, 497 drug suspects had been arrested, several property confiscated and weapons worth US$250 million were recovered. In retaliation, a total number of 187 civilians and government officials were murdered by 'coke' princes, 265 bombings were carried out and property estimated at over US$500 million were destroyed (Times Magazine, 18 December 1989: 26).

SELF ASSESSMENT EXERCISE

Explain any four aspects of terrorism.

3.3   **Individual Protective Measures**

a) It is important to be alert and take a good watch of the surrounding area and quickly respond when you see some suspected people that you consider can 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 a 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 loads that you are not sure of their contents from people especially the strangers, not for any amount. The reason is that the cost of damage that you may suffer for accepting such loads 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 case of emergency situation that may be occasioned by terrorist attack;

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;

g) In the event of terrorist attack, you should be calm and avoid anxiety because anxiety can deprive you opportunity to respond creatively and effectively to mitigate the impact of the hazard on you;

h) Quickly inform the law enforcement agents of the terrorist attack and notify 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;

i) Carefully, locate the emergency routes through which you can negotiate your escape from the building under a terrorist attack;

j) 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 explosive(s) or dangerous materials like bio-chemical agents in the lift in which many people will lose their lives. It is therefore wise to carefully use the stairs and don't be panic to avoid stampeding;

k) There is need to use masks by the rescuers to avoid any form of chemical or biological attack from the hazard; and

l) 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.

4.0   CONCLUSION

By the 1960s, international terrorism assumed a level of modernism of more strategic and tactical characters. Its superficial sophistication is consequent upon emergent global variables like cold war, upsurge in nationalism, self determination insurgency, unresolved conflict between Palestine and Israel, Coups and Counter Coups, economic

depression, Islamic fundamentalism, revolution in technology and communication among others.

The strategy, tactics and operators of modern terrorism are totally not consistent with the 19th century terrorism. Prior to the later part of the 20th century, the doctrine of mass destruction and violent recklessness that dominate modern terrorism was palpably absent (see Jenkins, 1975: 8). Proliferation of weapons and technological advancement brought into the fore by cold war as well as cacophonic international media coverage of international terrorism had really altered the traditional philosophy of international terror. Most unfortunately, mass destruction has become object of international recognition and yardstick to measure the success of any terrorist network.

5.0   SUMMARY

In this unit, our focus was shifted to another human form of security threat. We began the study by explaining the meaning of terrorism. Thereafter, we presented various forms of terrorism, and our attention was also drawn to various aspects of terrorism. The last area of discourse was a list of individual protective measures or actions, which can help us to mitigate the incidence of terrorism.

6.0   TUTOR-MARKED ASSIGNMENT

Describe the term terrorism, and mention any four aspects and forms of terrorism.

7.0   REFERENCES AND FURTHER READING

Berkowitz, B. J., Frost, M., Hajic, E. J. & Redisch, H. (1972). *Superviolence: The Civil Threat of Mass Destruction Weapons*. Report A72-034-10, 29 September. ADCON (Advanced Concepts Research) Corporation, Santa Barbara, CA.

Claude Jr., I. L. (1980). Just Wars: Doctrines and Institutions. In Connery, R.H. & Caraley, D. (eds). *National Security and Nuclear Strategy*. New York: The Academy of Political Science. 83-96.

Hardman, J.N. (1937). Terrorism in 14 *Encyclopedia of the Social Sciences*, New York: Macmillan. 575 – 579.

Higgins, R. (1997). The General International Law of Terrorism. In Higgins, R. & Flory, M. (eds). *Terrorism and International Law.* London: Routledge. 13-42

Jenkins, B. M. (1975). *High Technology Terrorism and Surrogate War: The Impact of New Technology on Level Violence*, (The RAND Paper Series, No. 5339) January.

Times Magazine (18 December 1989).

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

Wardlaw, G. (1989). *Political Terrorism: Theory, Tactics and counter measures* Cambridge University Press.

://en.wikipedia.org/wiki/Bioterrorism. Retrieved on 28 October, 2009.

.atomicarchive.com/Glossary/Glossary8.shtml. Retrieved on 30 October, 2009.

://www.dawn.com/weekly/dmag/archive/020616/dmag21.htm). Retrieved on 30 August, 2008.

://edhelper.com/Reading_Comprehension_33_243.html. Retrieved on 30 October, 2009.

://www.guardian.co.uk/world/2005/mar/04/aids. Retrieved on 28 October, 2009.

://www.hhs.gov/disasters/emergency/manmadedisasters/bioterorism/index.html. Retrieved on 28 October, 2009.

://www.medterms.com/script/main/art.asp?articlekey=18694. Retrieved on 8 October, 2009.

.nmmems.org/main_glossary_C.html. Retrieved on 10 October, 2009.
://www.nti.org/h_learnmore/radtutorial/chapter01_05.html. Retrieved on 30 October, 2009.

.pbs.org/wgbh/rxforsurvival/glossary.html. Retrieved on 28 October, 2009.

://www.stimson.org/pub.cfm?ID=472. Retrieved on 29 September, 2009.

UNIT 4

WAR AS A SECURITY THREAT

CONTENTS
1.0　　Introduction

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 shift in paradigm in the analysis of security issues in recent time. 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, due to the demise of the Cold War, 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 the emerging security threats has been a source of worry not only 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 potentials of countries like Nigeria to effectively manage internal security, reducing the capacity of the government to achieving 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 Bauchi states where some anti-Western education Muslim jingoists engaged the security agents in bloody battle, a situation that led to more than 1000 deaths, is worthy of note.

The unprofessional handling of the situation by the Nigeria Police raised a doubt about its capacity to manage crime and overall internal security of the country. If the excesses of the *Boko Haram* sect were not checked by the law enforcement agents (especially the Army), the group may later decide to engage Nigerian state in "holy" war as a way of challenging its secularity. In this unit, we shall study 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 are rarely examined' (Smith, 1989:23). 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. The conceptualisation of war has remained problematic in international relations. It has been greatly flexible and dynamic. Thus, there exist specific parameters to define the concept of war. According to Adeniran (1982), 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 with. 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 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 will you describe the term war?

3.2   **Features of War as a Security Threat**

The experience of the 20th century has shown that the century recorded more war with incomparable human casualty than the 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 Nwolise (2004) 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 of 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, 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 but many 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 their second nature.

The 1999 Lomé Agreement failed to restore any peace to the country due to the strategic advantage it gave to 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. The 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. The 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, 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 not surprising that anybody who is recruited into the military must be physically fit and be emotionally stable. War is not a joke, it is a serious business!

There are some light weapons that ordinary a man cannot carry. Not every adult can withstand operating an AK-47 riffle because of the pressure it exerts. Not only 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 object at work.

Also, war consumes a lot of socio-economic resources. In the 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, an 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 power and a weak nation, considering the military capability and mobility, and strategic superiority enjoyed by the former over the latter, the former (great power) would be victorious.

Carl Von Clausewitz disagreed with the above notion, arguing that war is not only a risky business but 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 to win 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 basis by the local militants through guerrilla war strategy is considerably high.

Another example of uncertainty in the outcome of war was 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 was 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, 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 the undefined cause of events not subject to calculation. According to Clausewitz, 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 an enthusiasm or zeal for a while 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. Her mission was basically to wrestle political power from the portuguese colonialists for 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 that 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 the activities of Germany after the First World War. Germany was sanctioned and faced a great penalty for war-mongering. But 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 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, we mean 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 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 soldiers from Iraq's side that survived the military onslaught by the allied forces thereby 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, the rise of nationalist struggle and rebellion has been phenomenal in developing countries especially 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 has remained a nightmare to Africa and the world at large. Nevertheless, 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, and security practitioners alongside other security stakeholders need to brainstorm and make collaborative efforts in the development of strategies in mitigating war and reduce losses that a warring situation may attract.

5.0   SUMMARY

In this unit, we discussed the meaning of war and showed how it constitutes a threat to the 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. The third and last area of discourse on the subject was to explain the basic categories of warfare: conventional and unconventional. Thank you for your patience and the zeal you have demonstrated to acquire knowledge since the beginning of this unit.

6.0   TUTOR-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.

UNIT 5

INFORMATION WARFARE AS A SECURITY THREAT

CONTENTS

1.0   Introduction
2.0   Objectives

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 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 beaming our search-light also on various types of information warfare. Thank you in anticipation of 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 constitutes a security threat; and

•   Identify types of information warfare

3.0   MAIN BODY

3.1   Describing Information Warfare

Traditionally, parties strived 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 thus:

Attaining 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 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 are 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 a 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:

any 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:

actions 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, information warfare has begun to receive growing interest among scholars in the field of security studies and policy makers due to its ability to destroy 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 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 the automobile industry. The US would manufacture a car model while China will do its imitation with improved quality, may even sell it at a cheaper rate, forcing buyers including Americans to rush for the China products. Due to the emergent information revolution that characterises 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 constitute 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 disgruntled elements like (adventurous) computer science students, hackers, despicable

programmers and some nefarious computer corporations. But, 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 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 or 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 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 was 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 not surprising that in an attempt by the US to contain the security threat that the activities of hackers pose 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, but James Adams, a Washington based journalist revealed, after

conducting a number of (secret) interviews for several senior officials of the Pentagon. According to him:

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. Such amount of money is far greater than the annual budgets of several countries in Africa and elsewhere; and

d)   Physical Attacks: 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 .iwar.org.uk/ iwar/resources/nato/as 285 stc-e.html).

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 the 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, hacking etc. Some of the ways through which we can mitigate information warfare shall be explained subsequently (in module 3).

6.0 TUTOR-MARKED ASSIGNMENT

Define 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.

://w.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.

MODULE 2 ANALYSIS OF NON-HUMAN SECURITY THREATS

Unit 1:   Analysis of Geological Security Threat/Hazards I
Unit 2:   Analysis of Geological Security Threat/Hazards II
Unit 3:   Analysis of Climatic Security Threat/Hazards
Unit 4:   Analysis of Environmental Security Threat/Hazards I

Unit 5:   Analysis of Environmental Security Threat/Hazards II

UNIT 1

ANALYSIS OF GEOLOGICAL SECURITY THREATS/HAZARDS I

CONTENTS

1.0.   INTRODUCTION

There are various types of security threats but they can be summarised into human and non-human threats to security. These non-human security threats can also be classified into three including geological hazards or threats, climatic hazards or threats, environmental hazards or threats. Epidemics and pandemics, and industrial accidents can be described as both natural and human. Meanwhile, it is generally believed in some quarters that all these non-human or simply natural hazards/threats usually have human activities contributing to their occurrence in one way or the other.

For instance, deforestation is an environmentally hazardous situation that is usually created by some activities of man like felling of trees and bush burning. In this unit, our focus shall be centred on the analysis of two of the geological security threats or hazards: tsunami and earthquake. It is as a result of the limited time and space we have in this unit that we will not be able to cover the other two geological hazards (volcanic eruption and landslide), which we shall beam our searchlight on in the subsequent unit of this course.

2.0   OBJECTIVES

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

Discuss and analyse tsunami as a geological type of natural security threat or hazard; and

Explain and analyse earthquake as a form of geological security threat or hazard.

3.0   MAIN BODY

3.1   Analysing Tsunami as a Geological Hazard/Threat

Etymologically, the word "tsunami" emanates from the Japanese meaning "tsu" (harbour) and "name" (wave). Tsunami can be described as massive waves around the harbour capable of causing enormous destruction to lives and property. Tsunami constitutes great security threat to man and his environment, and resulting from its very adverse effect and highly destructive consequences often occasioned by its occurrence, it has continued to attract growing interest among scholars especially in geography, geology, environmental science, and security studies. Through various intellectual works and research inquiries about the subject (tsunami), many definitions of the term have emerged. Though, the list of these definitions is very long and endless but we shall be considering some of the available definitions in our conceptual description of the term. Therefore, tsunami can be defined as:

...waves characterized by moving at fast speeds, sometimes having a high amplitude (wave height), and long wavelength – thus tsunamis are essentially giant waves. In the deep ocean, tsunamis are barely felt since they are masked by the sheer vastness of the rest of the ocean...The speed at which a tsunami travels is another impressive characteristic. Tsunamis can travel at great speeds across an ocean, usually from 500 to 1000 kilometres per hour, with hardly any energy losses and are barely noticeable out at sea. This is the reason why tsunamis generated from one region can affect other regions thousands of kilometres away (://www.ringsurf.com/ online/2410-what_is_a_tsunami_.html).

...a series of large waves of extremely long wavelength and period usually generated by a violent, impulsive undersea disturbance or activity near the coast or in the ocean. When a sudden displacement of a large volume of water occurs, or if the sea floor is suddenly raised or dropped by an earthquake, big tsunami waves can be formed by forces of gravity. Earthquakes, landslides, volcanic eruptions, explosions, and even the impact of cosmic bodies, such as meteorites, can generate tsunamis. Tsunamis can savagely attack coastlines, causing devastating property damage and loss of life (://www.kjc.gov.my/english/education/seismology/whatistsunami.html).

Tsunami is usually mounted by some geological conditions like earthquake, landslides and volcanic eruptions as well as under-water explosions like detonations of nuclear devices at sea among others (see ://en.wikipedia.org.wiki.Tsunami). Tsunami waves are usually more or less noticeable in deep water and its measurement can show a travel speed of 160km between wave crests (UNDP & UNDRO, 1992: 35). Another feature or characteristic of tsunami is that it may consist of ten or more wave crests. There is doubt no that tsunami is very devastating and destructive to human, physical and other forms of security considering its damaging effect on man and the

environment. And some of these effects or consequences posed by the incidence of tsunami to any community shall be explained subsequently.

3.1.1 Effects of Tsunami

i. Destructive waves speed: From the deep water of the ocean, tsunami moves at considerably very high speed into the shallower water close to the coast, causing devastating destruction to lives and property when it approaches the land. In the deep water, it often appears like normal wave but it moves at very fast rate, and its power becomes tremendously amplified with its long wavelength, pilling up water to increase its height to as high as 30 meters when it finally reaches the land. Consequently, it can shred sand from beaches and cause extensive damage to mankind and environment as shown in the South Asian tsunami tragedy (see ://www.ringsurf.com/online /2410-what_is_a_tsunami_.ht ml);

ii. Flooding: Another effect of tsunami is mounting of flood. It has the potential of causing flood, increasing the water level by hundreds of meters, which will move at a very fast rate capable of destroying homes and any other structures offshore as well as endangering the lives of the affected inhabitants resulting in many deaths (see ://www.kjc.gov.my/english /education/seismology/whatistsunami.html);

iii. Extensive damage to human beings and physical structures: As we have pointed out earlier, tsunami has capability to increase sporadically and swiftly the level of typical water in the affected community, generating flood. The water force is usually overwhelming with strong capacity to demolish structure that comes in contact with it;

iv. Casualties and public health: The phenomenon of tsunami always occasions the incidence of drowning that consumes many lives. Apart from drowning, the physical infrastructure or facilities destroyed by the tsunami can also cause injuries and deaths when being tattered by debris (UNDP & UNDRO, 1992: 35). The affected community suffers greater risk of disease epidemics that can potentially force the public health to its knees especially through the decomposing dead bodies;

v. (Acute) water shortage: Tsunami can also create a situation of acute shortage of drinking water. The destruction to infrastructures and physical structures can infest water facilities to germs and bacteria increasing the chances of plaguing the affected community with water-borne diseases. For instance, the sewage system may have got damaged and the wastes running into the water facilities, and in a situation like that, there is high probability that there will be epidemics of cholera and other water-borne diseases if people drink such contaminated water. There is the likelihood that such situation will lead to more deaths; and

vi. Food shortage: Due to very destructive nature of tsunami, the harvests, food stocks, live-stocks and agricultural facilities can be destroyed by the tsunami waves causing widespread food shortage to the affected community. This will, therefore, affect the capacity of the affected community to ensure any food security to its people for some time. But in communities where largely, there is absence of adequate disaster mitigation measures and practices, it may take a very long time to recover from such food shortage, if they ever get out of it.

3.1.2 Predictability

Tsunami cannot be adequately predicted because of the very little warning signal it gives before it strikes. Though, the Tsunami Warning System in Pacific has been very helpful in monitoring seismic activity and it alerts on the probable occurrence of tsunami but the waves mounted by earthquake may quickly smack the nearby shores and within very short time the tsunami waves may hit the coastal areas, providing very little or no opportunity to alert the public to embark on evacuation immediately (see UNDP & UNDRO, 1992: 35).

3.1.3. Vulnerability

The experience of tsunami in a community is largely hinged on a number of contributory factors which include:

i.   Location of Communities: The issue is that those communities in low lying coastal regions always appear to be more vulnerable to the incidence of tsunami;

ii. Another factor is absence of mitigation measures and preparedness. For instance, in several communities situated on low lying regions, we still have buildings being erected without fortifying such buildings with tsunami resistance materials;

iii. Ability of any community to issue warning and notification about hazardous events will largely determine its capacity to reduce the effect of such hazardous incidents on its people and environment. Those communities that have no public alert or warning systems to promptly and adequately notify the people are more likely to record higher casualty rate than those communities that have effective warning systems. Again, preparedness is also vital for hazard mitigation, and where there is lack of adequate evacuation plans, there is tendency that such communities will be more vulnerable to hazardous events like tsunami;

iv. Communities that fail to educate its people on security risk and disaster reduction are likely to experience more devastation from the incidence of

tsunami and other hazardous events because people have no knowledge of how to act creatively and effectively in mitigating the effect of hazards on them; and

v.   Communities that have little or no protective plans are more vulnerable to hazards like tsunami and suffer more destructions than those communities with appropriate protective plans.

3.1.4 Risk reduction and preparedness measures

The following risk reduction and preparedness measures can assist:

i.   Fortifying the houses near the coasts with tsunami reduction materials;

ii.   Erection of water barriers including break waters to reduce the force of water created by flood engineered by tsunami (UNDP & UNDRO, 1992: 35). This action is likely to reduce the level of damage that may be propelled by tsunami incident;

iii.   Hazard mapping is also essential in mitigating the impact of any hazardous situation on the people in any given community. Through hazard mapping we will be able to identify potential hazards, their patterns and trends as well as the level of threat they constitute to the wellbeing of the community at large;

iv.   Evacuation plans are also very important to enhance the capacity of any community in mitigating or reducing the impact of hazardous events like tsunami. It is very germane to have effective preparedness plans by creating sufficient evacuation exits through which people can escape the onslaught that may be occasioned by any hazardous events like tsunami. It is also important to educate people on protective actions that they can undertake to reduce the effect of hazardous situations like tsunami; and

v.   Putting in place effective warning systems can also be helpful in providing prompt notification and alert to the public whenever it is noticeable that tsunami waves are approaching the coast. This will enable people to prepare themselves against the impending hazard. If the waves give opportunity for quick evacuation, people can then exit the affected place without wasting time because each minute counts in reducing the devastating effect of tsunami.

3.1.5. Impact assessment techniques

In analysing the incidence of tsunami as a threat, it is important to conduct assessments of the hazardous situation with the use of a number of techniques that include:

i.   Aerial surveys of all areas or communities close to coasts;

ii.   Damage surveys to determine the level of damage associated with the hazardous situation; and

iii.   Evaluations of public warning and alert systems and evacuation plans to measure level of community's vulnerability to the hazard and its preparedness towards hazard mitigation.

3.1.6. **Individual safety measures**

i.   If one is at home, he/she is expected to inform the people around including his/her family and neighbours immediately he/she hears the public warning about tsunami or any other occurring hazard, so that they will become aware of the situation at hand. This will afford them the opportunity to prepare themselves against the hazardous situation and act promptly if there are evacuation plans.

Meanwhile, due to the nature of tsunami, giving little or no time to embark on public evacuation of the affected areas, it is important for individuals to move to parts of their houses where no heavy objects can fall on them resulting from the force of the waves or water;

ii.   If one is outside, look for a place where no heavy structures or materials like electric poles or cables or trees etc can collapse on you to avoid sustaining injuries that may make you unconscious or die or even electrocuted;

iii. Drawbacks can also be very useful in providing brief warnings to people when tsunami waves are approaching the land. Drawback is usually experienced before the occurrence of tsunami. It occurs due to the fact that "tectonic plate on one side of the fault line sinks suddenly during the earthquake, causing the overlaying water to propagate outwards with the trough of the wave at its front" (://en.wikipedia.org/wiki/Tsunami). For instance, in 2004, a ten-year old girl, Tilly Smith who resided in Surrey, England, through lessons given to her about tsunami by her geography teacher, Mr. Andrew Kearney, saved the lives of many people.

Little Tilly was on Maikhao beach in Phuket, Thailand with her parents and sister when she noticed some drawbacks which signified that tsunami waves were approaching the coast, and she alerted her parents. Immediately, the parents notified the people that tsunami was most likely to occur very soon, saving the lives of many on the beach. It is also important to note that in some exceptional cases, drawbacks are not experienced and the people will be caught unaware by tsunami as evident in the 2004 Indian Ocean tsunami whereby there was no drawback on African and some other eastern coasts that were also hit by the tsunami, largely for the reason that the "wave moved downwards on

the eastern side of the fault line and upwards on the western side" (://en.wikipedia.org/wiki/Tsunami).

iv.   If one is on the beach a vibration of the land is noticed, you should make sure that other people are alerted promptly and proceed immediately to higher ground without waiting for tsunami warning (://www.kjc.gov.my/english/ education/seismology/whatistsunami.html).

v.   Whenever a public warning is issued about tsunami, if you are not at home, make sure you immediately look for a building and move to the topmost floor of the building.

vi.   If you are on board of a ship or boat when you get an alert about the occurrence of tsunami, avoid sailing to the port because tsunami waves can potentially "...cause rapid changes in water level and unpredictable dangerous current in harbours and ports" (://www.kjc.gov.my/english/education/seismology/ whatistsunami.html), which can pose a great danger to the lives of those on board.

SELF ASSESSMENT EXERCISE

How do you analyse tsunami as a security threat?

3.2   **Analysing Earthquake as a Geological Hazard/Threat**

Mythologically, earthquake was believed among the Greek to be caused by Poseidon who was the god of earthquake. It was argued by the 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 also claimed that this god also used earthquake as a tool of fear, warning people of the damaging effect that 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. The 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 referred to as the "epicentre" (://en.wikipedia.org/wiki/Earthquake).

One unique character about earthquake is that it does not constitute any danger to people or animals on its own, but its consequences such as collapse of building, felling of electric poles, electric shock, fire, to mention a few that usually cause harm to people. This means that it is imperative to have safety measures in place and encourage hazard mitigation 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 the 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 may 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.

3.2.1 **Effects of Earthquake**

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:

i.   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](://www.abag.ca.gov/bayarea/eqmaps/doc/contents.html)). However, ground acceleration is often used in measuring the degree of ground shaking;

ii.   Fires: Another effect that can be caused by earthquake is 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 fell electric-pole and damage power-lines, and in the process, the spark that may come from the power-line or electric-poles may have contact with gas or petrol to generate fire. The pressure of these fires may be so high that it will be very difficult to contain them. An example of where the earthquake caused lesser threat than its fire outbreak effect was the 1906 San Francisco earthquake where many people died as a result of fires that accompanied the earthquake incident (see **Error! Hyperlink reference not valid.**);

iii. Soil liquefaction: One of the 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 its 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 as experienced in the 1964 Alaska earthquake (**Error! Hyperlink reference not valid.**); and

iv. 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.

3.2.2 Predictability

Earthquake cannot be adequately predicted but there are scientific approaches through which its occurrence can be determined based on probability with very little or no precision about the timing of the occurrence. Forecasting can be useful in observing seismic activity and historical incidence to determine the susceptibility of any community to the incidence of earthquake (see UNDP & UNDRO, 1992: 34).

3.2.3 Vulnerability

i. The location of the community usually determines its vulnerability to earthquake. The reason is that those communities found on the seismic areas are prone to experience earthquake;

ii. In the settlements that lie on seismic areas, it is imperative to ensure that houses are built in such a way that they will be resistant to ground vibration that will be occasioned by the quake of the earth. In those communities where people build or erect buildings without appreciating the importance of fortifying their buildings in such a way that they can resist being submerged by the ground motion or vibration that will be generated by earthquake, shows that such communities will be much vulnerable to the incidence of earthquake. Hence, the probability of recording high casualty and physical destruction rate resulting from the incidence of earthquake will be high in such communities;

iii. Communities especially those considered densely populated settlements that are found in the seismic areas where there is high occupancy of buildings are more vulnerable to incidence of earthquake. Due to high rent requests, buildings will just be erected anyhow especially in those places where little or no importance is given to physical planning in order to accommodate most (prospective) house seekers. This will further create tension on the land;

iv.   Risk education and knowledge about hazards should be given to the public, and where the people have very little or no knowledge about risk and hazard, there is tendency that such communities will become vulnerable to hazards including earthquake. The reason is that many of the people due to their lack of risk education will not be able to act adequately well when confronted with hazardous events like earthquake; and

v.   Absence of effective public warning system makes any community vulnerable to hazardous events or threats.

3.2.4. **Risk reduction and preparedness measures**

i.   Hazard mapping can assist in no small measure to reduce the effect that the occurrence of earthquake can have on any community. Through hazard mapping we will be able to identify potential hazards, their patterns and trends as well as the level of threat they constitute to the wellbeing of the community at large. Again, hazard mapping guide us in making right decisions regarding the way we can mitigate hazards like earthquake. For instance, by mapping hazards, we will be able to identify which communities that are in seismic areas (thereby being prone to earthquake) and ensure that buildings are not erected anyhow to reduce the incidence of building collapse resulting from the vibration that often characterises earthquake;

ii.   Evacuation plans are also very important to enhance the capacity of any community in mitigating the impact of hazardous events like earthquake or/and reducing the losses that may accompany any hazardous situations like earthquake;

iii.   Public awareness about hazards and mitigation strategies should be promoted, so that people will find it easy to act effectively, promptly and adequately on their own in responding to hazardous situations or threat;

iv.   There should be effective warning systems to alert and notify the public of the occurrence of any hazardous events like earthquake;

v.   There should be adequate evacuation plans.

3.2.5. **Impact assessment techniques**

The basic impact assessment tools for earthquake include earthquake scales (Modified Mercalli, MSK) as well as earthquake damage and usability forms.

3.2.6. **Individual safety measures**

i.   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;

ii.   It is imperative to educate the public on how to manage their home appliances and build in themselves culture of safety like switching off electricity or/and gas cooker or/and electrical appliances when they 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.

iii. 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;

iv.   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 loud sound that usually indicates the arrival of an earthquake. You are only left with very little or no time to prepare yourself 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 impact on you and those around you. Steps to take should include;

v.   You should take cover by looking for a very safe place where you can veil yourself against any falling objects like wall, ceiling fan, etc. It is advisable to lie under a table or well-built furniture, and you should also make sure that the furniture are well positioned to prevent it from being stumbled;

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

vii.   If you find yourself in a tall building, you should avoid using the lift to get out of that building. It is advisable 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;

viii.   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;

ix.   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;

x.   After the incident of earthquake, resulting from the presence of debris in the aftermath of earthquake, you are advised to wear cover shoes to avoid your foot being exposed to any dangerous particles or sharp objects that may get you injured or infected with a disease;

xi.   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;

xii.   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;

SELF ASSESSMENT EXERCISE

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

4.0   CONCLUSION

There is no doubt 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 possibility that such hazard will result in disaster.

5.0   SUMMARY

In this unit, we have been able to cover two of the major geological hazards or threats: tsunami and earthquake. We began the study by examining the meaning of tsunami and we proceeded to analyse the subject (tsunami) by looking at several issues concerning it including its effects, its predictability etc. Thereafter, we defined earthquake and analysed it as well by examining those issues that bother on its effects, predictability, vulnerability of communities to it, how its impact on environment and people can be mitigated, its impact assessment techniques and finally the safety measures that can be taken by individuals to reduce its adverse effect on them and their communities. It is my belief that you have found this unit very thought-provoking and intellectually stimulating.

6.0   TUTOR-MARKED ASSIGNMENT

Analyse tsunami and earthquake as geological forms of security threats or hazards.

7.0   REFERENCES AND FURTHER READING

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

UNDP & UNDRO (1992). *An Overview of Disaster Management* (2nd Edition). Disaster Management Training Programme.

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

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

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

://en.wikipedia.org.wiki.Tsunami. Retrieved on 5 September, 2009.

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

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

://www.kjc.gov.my/english/education/seismology/whatistsunami.html. Retrieved on 6 September, 2009.

Error! Hyperlink reference not valid.. Retrieved on 6 September, 2009.

UNIT 2

ANALYSIS OF GEOLOGICAL SECURITY THREATS/HAZARDS II

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Body
      3.1   Analysing Landslide as a Geological Hazard/Threat
      3.2   Analysing Volcanic Eruption as a Geological Hazard/Threat

1.0.   INTRODUCTION

In the previous lesson or unit, we focused on the analysis of two of the basic types of geological security threat or hazard: tsunami and earthquake. We explained their meaning, their effects on any people or community that experience them. We also discussed various factors or conditions that often make any community or people vulnerable to those hazardous events as well as some other issues that bother on the analysis of the risk posed by those threats to the wellbeing and survival of any community.

In this unit, we shall continue from we stopped in the last unit, and thereby we shall discuss another set of geological security threats or hazards including landslide and volcanic eruption. Undoubtedly, geological forms of threat or hazard usually have very adverse impact on man and general ecosystem due to the high level of destructions in human and material terms that often characterise their occurrence. For instance, in the 2004 Indian Ocean tsunami episode, no less that 200,000 people were reported killed while more than 1 million people lost their shelter and/or means of livelihood. Another example is the November 9, 2001 Amboori debris flow (landslide) incident in Kerala, India, killing no less than 39 people (see Kuriakose *et al.* 2008).

Apart from destruction of human lives and property, geological hazards can impose acute food shortage or food insecurity on any affected community due to extensive damage of livestocks, harvest, plantations, and food storage facilities. It is as a result of the mammoth negative implications that these geological threats or hazards have on the continued survival of any community and development that many state and non-state actors have been creating frameworks through which they can mitigate or reduce the impact of these hazardous events. For instance, an incident of earthquake can wipe-out in minutes the development that has taken a community several years to accomplish. In furtherance of our study on the geological forms of threat, we shall beam our searchlight on landslide and volcanic eruption.

2.0.   OBJECTIVES

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

- Explain the meaning of landslide;

- Analyse landslide as a form of geological security threat or hazard;

- Describe volcanic eruption; and

- Examine volcanic eruption as a geological type of threat or hazard.

3.0.   MAIN BODY

3.1   Analysing Landslide as a Geological Hazard/Threat

Landslide is another form of geological hazard. It is a natural security threat that can pose serious risk to any people or community. It also involves mud flows, debris flows, earth failures among other geological conditions, and it is usually caused by rain, floods, earthquakes among other natural causes. Apart from the natural causes, there are several human factors that can also contribute to the incidence of landslide, and these include grading, terrain cutting and filling, over development of an area among others.

Landslide has been occurring in the world since the prehistoric time and an example of the recorded incidents of landslide in prehistoric time was the Ruatoria debris avalanche off North Island New Zealand, which was calculated at 3,000 km³ in volume and occurred 170,000 years ago (Kuriakose, Sankarm & Muraleedharan, 2008). How do we define landslide? Simply, landslide can be defined as:

…rock, earth, or debris flows on slopes due to gravity. They can occur on any terrain given the right conditions of soil, moisture, and the angle of slope. Integral to the natural process of the earth's surface geology, landslides serve to redistribute soil and sediments in a process that can be in abrupt collapses or in slow gradual slides. Such is the nature of the earth's surface dynamics (://www.ussartf.org/ landslides.htm).

…(or landslip) is a geological phenomenon which includes a wide range of ground movement, such as rock falls, deep failure of slopes and shallow debris flows, which can occur in offshore, coastal and onshore environments (**Error! Hyperlink reference not valid.**).

A natural disaster that involves the breakup and downhill flow of rock, mud, water and anything caught in the path (://en.wiktionary.org/wiki/landslide).
A sudden movement of rock and soil down a slope (.macmillanmh.com/ science/2008/student/na/grade4/glossary/l.html).

Downward movement of a slope and materials under the force of gravity (.ak-prepared.com/plans/word_docs/StateHazardMitigationPlan07/07%20SHRMP%20Appendices/Appendix_2_Definitions.doc).

3.1.1.   Effects of Landslide

i.   Physical destruction: The amount of damage to infrastructure and other physical facilities can be very devastating, and capable of overwhelming the capacity of any affected community to sustain its development. Through the

attendant destructions occasioned by landslides, the affected community may experience collapse of bridge(s), poles carrying telecommunication and electric cables, rubbles adorning the streets capable of blocking the roads and affecting traffic flow, among other physical damages;

ii.   Food insecurity: Landslides can potentially reduce the capacity of the affected communities to feed themselves due to possible extensive damage that landslides might have inflicted on the livestock, food storage facilities, harvest as well as plantings. Landslides can cause flooding and reduction in agricultural productivity;

iii.   Casualties: Landslides can lead to the death of many people and can also cause various degrees of injury among the affected people. Slope failures and mudflows can cause high fatality as many people can be buried by the rubbles; and

iv.   Distortion of development: Resulting from the devastating damage that landslide inflicts on physical structures and infrastructure of any affected community, it retards the development of that community. For instance, an incident of landslide can bring down houses and infrastructure like bridge, shopping mall, office buildings, recreation centres, communication facilities, power lines among others social infrastructure, that may have taken the affected community decades to attain, within a few hours or even minutes.

3.1.2 Predictability

There is no doubt that landslide occurs more than any other geological hazards or threats. It has many forms of movement including falls, slides, topples, lateral spread, and flows. It can also occur as secondary effects of earthquakes, volcanic eruption as well as heavy storms. On the question of its predictability, environmental scientists and disaster management experts rely largely on information gathered on the frequency of its occurrence as well as its extent and effects to determine those communities or communities that are susceptible to landslide. Experts arrive at their decision in identifying the communities that are at greater risk of incidence of landslide by looking also at the geology, geomorphology, hydrology and climatology, and vegetation of the communities.

3.1.3. Vulnerability

The factors that contribute to the vulnerability of any community to landslide may include:

i.   The location of a community largely determines how vulnerable it will be to the incidence of landslide. The communities that are sited on steep slopes or softer soil or cliff tops are usually vulnerable to landslides;

ii.   Studies have also shown that those communities that are sited on the base of steep slopes or on mouths of streams near the mountain valleys are vulnerable to landslides (UNDP & UNDRO, 1992: 37);

iii.   The buildings erected, the roads built and the communication lines mounted in mountain areas can also experience landslides;

iv.   The buildings without any solid foundation may also be vulnerable to landslides; and

v.   Communities with very little or no hazard mitigation education are always vulnerable not only to landslide but also other hazardous events because they will exhibit low preparedness attitude and recovery capacity in responding to hazardous situations or attacks such that such threats can easily lead into disasters.

3.1.4   Risk reduction and preparedness measures

i.   Geographic Information Systems (GIS) can be a very important tool in the mitigation of landslide because it allows us to collect, store, manipulate, display and analyse a wide-spectrum of spatially referenced data very adequately and effectively (Clerici *et al.* 2002: 8);

ii.   Hazard analysis and mapping is very vital in mitigating landslides by providing us relevant information on ways to reduce the adverse impact that landslide may have on any people or community. It also enables us to develop framework and policy decisions for sustainable land use planning. Again, through this technique we can identify the factors that contribute to the incidence of landslide and measure how much each of the factors contribute to landslide through which we can establish relation among the factors with the aim to making prediction about future occurrence of landslide (Chen & Wang, 2007);

iii.   The use of satellite imagery along with GIS can also assist us to reduce the adverse effect of landslide because it allows us to create maps regarding the possible occurrence of landslides in future (Fabbri et al, 2003). Through generation of maps, communities that experience or are likely to experience landslides will step-up their preparedness towards mitigation of this hazardous situation. With the use of the maps produced by satellite imagery, we shall be able to identify locations where previous incidents of landslide have taken place and show the locations where future landslides will probably occur.

However, by establishing relationship between previous events of landslide and locations of possible future hazardous events of landslide, we shall be able to predict using some geologic factors especially geomorphology, land use and hydrogeology (see Clerici et al., 2002) as well as lithology to determine those

locations that will most likely experience landslides in future for exhibiting similar conditions that characterised past events of landslide (Lee & Talib, 2005);

iv.   Risk education is also important in reducing the effects of landslides on any community or people. It assists to increase the consciousness of any people towards improving their preparedness and it also enhances their capacity to act creatively, promptly and effectively when confronted with any hazardous situations like landslide such that the masses can respond on their own without waiting for emergency workers or security practitioners; and

v.   There should be regular evaluation of monitoring, warning and alert systems to test their effectiveness and in ensuring their optimal performance.

SELF ASSESSMENT EXERCISE

How do you analyse landslide as a form of geological hazard ot threat?

3.2   **Analysing Volcanic Eruption as a Geological Hazard/Threat**

Volcanic eruption is another form of geological hazard or threat. According to Fank & Wagnalls Standard Dictionary, volcanic eruption can be described as a hazardous event that involves:

...an opening in the earth's surface surrounded by an accumulation of ejected material, forming a hill or mountain, from which heated matter is or has been ejected.

Volcanic eruption can also be defined as a hazardous situation whereby:

Magma pushes upward through volcanic vent by pressure and effectiveness of dissolved gases (UNDP & UNDRO, 1992: 36).

There are several types of volcanic eruption, which include cindercones, shield volcanoes, composite volcanoes and lava domes. Whenever volcanic eruption occurs one of the fundamental features that it bears is gushing-out of magma to the surface and this is known as lava. Also, there are solid particles driven out resulting from the eruption, which are known as tephra. Usually, volcanic eruption constitutes a major security threat to any people or community through the destructive materials such as ash, pyroclastic flows, mud, debris as well as lava flows that it emits. These materials can destroy plants, infrastructure as well as cause serious injuries or death to human beings and animals.

3.2.1   **Effects of Volcanic Eruption**

i.   Destruction of infrastructure and physical facilities: One of the effects of volcanic eruption is widespread destruction of physical structures and infrastructure. The pyroclastic, lava flows or mud can destroy infrastructure;

ii. Casualty and public health hazard: Pyroclastic flows, mud flows and even lava flows as well as toxic gases which are produced by volcano are very capable of causing deaths to human beings and animals within the affected community or area. The amount of respiratory problems ejected by this hazard can be enormous, likely to cause deaths and respiratory ailments among the affected people. The decaying bodies of those who have died resulting from the hazardous event can cause epidemics and pose a huge challenge to public health of the affected community;

iii. Water shortage: Some of the destructive materials produced by volcano can also contaminate water capable of causing acute shortage of drinking water;

iv. Food insecurity: Volcano can also mount a situation of food shortage on the affected community. This hazardous event can destroy the plants, food storage facilities, harvest as well as cause great danger to livestock. The poisonous gases that it produces when inhaled can lead to the death of high number of livestock. Unless, there had been adequate mitigation measures, the community that experienced volcanic eruption was likely to experience the problem of food shortage; and

v.   The huge amount of destruction often occasioned by volcano usually undermines the development of the affected community. One of the reasons is that, rather than providing further development, the affected community will be grappling with ways through which it can replace the infrastructure and other developmental facilities destroyed as a result of the incident of volcanic eruption.

3.2.2 **Predictability**

The incidence of volcanic eruption cannot be adequately predicted. Meanwhile, studies on the history of phenomena of volcanoes on any areas or communities especially those located on the volcanic belt as well as seismic activity among other geological observations can assist us to identify and determine where future volcanoes are likely to be experienced.

3.2.3. **Vulnerability**

There are several factors that determine the vulnerability of any community or area to the incidence of volcanic eruption, and some of which include:

i.   The location of the community is one of the basic factors. The reason is that those communities or settlements that are located on the flanks of volcanoes will likely be more susceptible to volcanic eruption;

ii.   Another factor is that those communities or settlements that lie within historical paths of mud or lava flows will be vulnerable to volcanoes;

iii.   Those communities that lie on the volcanic belt where structures are erected or built without any consideration for designing their roofs in such a way that they can be resistant to ash accumulation (UNDP & UNDRO, 1992: 36);

iv.   Areas where there are explosive materials are likely to be much vulnerable in the occurrence of volcanoes. For instance, the areas that have the presence of large amount of weapons especially explosives will definitely experience greater amount of casualties and physical damage if volcano occurs. The fact is that the heated materials produced by volcano, apart from the destruction that they will cause to the affected communities or people, the explosives will also be triggered which will further complicate the hazardous situation. In a situation like this, it is more likely that such communities will have the hazard transiting or moving to disaster thereby leading to huge loss of lives and property;

v.   For communities especially those that are located on the volcanic belt where there are no adequate evacuation plans, the casualty rate and level of destruction will be high; and

vi.   In communities where there are no effective and adequate warning systems, there is high probability that such communities or settlement will be very vulnerable to any hazardous events including volcanic eruption. The reason is that most people will be unaware of the impeding danger, and before they know what is happening many of them must have been consumed by the hazardous event.

3.2.4 Risk reduction and preparedness measures

i.   One of the volcano mitigation measures is location planning. Through location planning, we will be able to map-out those areas considered close to volcano slopes, so that we will not allow important activities to take place there. For instance, it is not proper to cite trade centres anywhere without considering the geologic conditions of the areas.

Therefore, if an international trade complex is located in an area that is found on volcanic belt, apart from putting the lives of a large number of people (buyers and sellers) at risk, the huge amount of money spent in building such a

complex and various articles or commodities being traded will be put to a waste in the event of the occurrence of volcanic eruption;

ii.   Risk education is also important in mitigating the impact of volcanic eruption. Through risk education people will have enough awareness about the security risk posed by volcanoes and identify approaches and ways through which they can reduce the adverse effect such hazardous events may have on them individually and collectively. There is no doubt that through risk education, people's preparedness to act creatively and effectively against the hazardous situation will rapidly increase, so that they will be able to respond by reducing the losses that volcanoes can cause;

iii.   Evacuation plans are also very essential because it affords the communities where volcanoes are experienced to create routes through which affected people can be evacuated promptly and effectively to safer areas to reduce the loss of lives that such hazardous event can mount on them; and

iv.   Efforts can also be made to monitor volcanoes through which we can generate adequate information about volcanic activity. In providing this information to the people, there is tendency that their level of preparedness will increase such that they will be able to respond well in the occurrence of volcano by engaging in actions that can help to reduce the adverse impact that the hazardous situation can have on them.

3.2.5. Impact assessment techniques

i.   The ground and aerial surveys can be used to assess the impact of volcanoes;

ii.   Assessment of evacuation plans; and

iii. Capacity and vulnerability assessment can also be used to identify areas of weakness of any community in response to volcanic eruption and/or any other hazards.

3.2.6. Individual safety measures

xiii. One of the safety tips against volcanic eruption is to always ensure that your home is equipped 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. But it is more preferable to have transistor radio with ordinary batteries, which you can change to keep yourself updated as regards information concerning the volcano. It is important to know that rechargeable radio may disappoint if the battery current becomes emptied after a long use, thus, one cannot rule out total blackout during the occurrence of volcano and even shortly after it has lasted;

xiv.   It is also important to prepare yourself towards mitigating the effect of volcano on your household by identifying places in your house that can be used as cover in the event of emergence of volcanic eruption;

xv.   You should always have your phone fully charged and keep a 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 volcanic eruption. By doing this, you will enable your relatives and friends to monitor the state of your safety;

xvi.   Efforts should be made to fortify the house you are staying with roofs that are resistant to damage by volcanic materials;

xvii.   If you are outside when you get the notice about the hazardous event, make sure you locate a safe place to seek refuge or better negotiate for a safe evacuation route. It is always important to plan oneself against hazardous events by locating before-hand those exit points that can be considered as evacuation routes;

xviii. Make sure you keep a distance from windows, book shelves and sharp objects that can harm you when volcano occurs; and

xix.   After the incident of volcano, you should ensure that you and your household wear cover shoes to prevent your foot from being exposed to the harmful remnants of the volcanic materials.

SELF ASSESSMENT EXERCISE

How do you explain ways through which volcanic eruption can constitute threat to any people or communities?

4.0   CONCLUSION

From our discussion of various types of geological threat, it appears that these hazards including earthquake are very destructive and have the capacity to undermine the development of communities or people. It is more worrisome that these geological hazards can hardly be predicted but through some approaches and techniques, predictions can still be made about their future occurrence by considering the history of their occurrence, the geologic conditions among other observations of the communities that are considered prone to any of these hazards.

There is no doubt that these hazards have the tendency of transiting to disasters due to their rapid onset. They give little or no time for evacuation and for this reason it is important for any community to develop viable mitigation framework through which people can be promptly alerted or notified about any hazardous event. It is also important for every community to put in place adequate evacuation plans, hazard mapping initiatives, risk education, and other measures that can assist us in mitigating hazard and managing disaster.

5.0   SUMMARY

In this unit, we continued our study on geological forms or types of threat or hazard. Our first area of discourse was to look at the definition of landslide. In furtherance of our analytical dissection of the subject (landslide) we examined the adverse effects that it produces when it occurs in any community, and we also discussed other relevant issues including its (landslide) predictability, those factors that can make any community vulnerable to the incidence of landslide, risk reduction and preparedness strategies for hazard mitigation among others.

The second and last geological type of threat discussed was volcanic eruption. We began beaming our searchlight on the subject by defining it, and subsequently we analysed its various destructive effects and predictability. Thereafter, we explained those factors that make people or communities susceptible to volcanoes, some of the steps that can be taken to reduce the risk of the threat and people's preparedness towards reducing the losses that may accompany the occurrence of volcano among other issues. By and large, this unit can be considered to be interactive and communicative.

6.0   TUTOR-MARKED ASSIGNMENT

Describe landslide and volcanic eruption and list any three effects that each of them can have on people or communities.

7.0   REFERENCES AND FURTHER READING

Chen, Z. & Wang, J. (2007). Landslide Hazard Mapping using Logistic Regression Model in Mackenzie Valley, Canada. *Natural Hazards* 42:75-89.

Clerici, A., Perego, S., Tellini, C., & Vescavi, P. (2002). A Procedure for Landslide Susceptibility Zonation by the Conditional Analysis Method. *Geomorphology* 48(4):349-364.

Fabbri, A., Chung, C., Cendrero, A., & Remondo, J. (2003). Is Prediction of Future Landslides Possible with a GIS? *Natural Hazards* 30: 487-499.

Funk & Wagnalls Standard Dictionary (1962). International Edition. New York: Funk & Wagnalls.

Kuriakose, S.L., Sankar, G. & Muraleedharan, C. (2008). History of Landslide Susceptibility and a Chorology of Landslide Prone Areas in the Western Ghats of Kerala, India. *Environmental Geology*. Also available on **Error! Hyperlink reference not valid.**. Retrieved on 20 September, 2009.

Lee, S. & Talib, J.A. (2005). Probabilistic Landslide Susceptibility and Factor Effect Analysis. *Environmental Geology* 47: 982-990.

UNDP & UNDRO (1992). *An Overview of Disaster Management* (2nd Edition). Disaster Management Training Programme.

Error! Hyperlink reference not valid.. Retrieved on 10 October, 2009.

://en.wiktionary.org/wiki/landslide. Retrieved on October, 2009.

.ak-prepared.com/plans/word_docs/StateHazardMitigationPlan07/07%20SHRMP%20Appendices/Appendix_2_Definitions.doc. Retrieved on October, 2009.

.macmillanmh.com/science/2008/student/na/grade4/glossary/l.html. Retrieved on October, 2009.

://www.ussartf.org/landslides.htm. Retrieved on October, 2009.

UNIT 3

ANALYSIS OF CLIMATIC SECURITY THREATS/HAZARDS

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Body
      3.1   Analysing Hurricane as a Climatic Hazard/Threat

1.0   INTRODUCTION

The phenomena of hurricane, flood and drought have increased 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.

These climatic forms of security threat or hazard have adverse impact not only on man but also on general ecosystem. It is against this background that it is incumbent on every community and people to engage in actions that can mitigate the effect that the occurrences of these hazards may have on them and their environment by bringing into bear substantial measures to withstand the threat or hazard and reduce the human and material losses that may accompany their occurrence. In this unit, we shall analyse various climatic hazards and show how they constitute a threat to the security of any communities or people.

2.0   OBJECTIVES

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

• Define and analyse hurricane as a climatic hazard;

• Describe flood as one of the types of climatic security threat; and

• Explain the meaning of drought and show how it constitutes a threat as a climatic hazard.

3.0   MAIN BODY

3.1   Analysing Hurricane as a Climatic Hazard/Threat

In the last twenty years, there has been huge amount of losses in human and material terms through the 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" (**Error! Hyperlink reference**

not valid.). 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 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

3.1.1 **Effects of Hurricane**

i.   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;

ii.   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; and

iii. A storm surge actually involves a rise in 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 the hurricane strength" (**Error! Hyperlink reference not valid.**). 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	
2	155-178	96-110	2-3	6-8	
3	179-210	111-130	3-4	9-12	

| 4 | 211-250 | 131-155 | 4-6 | 13-18 | |
| 5 | >250 | >155 | >6 | >18 | |

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

3.1.2 **Predictability**

Hurricane can be predicted as landfall forecasts of its development can be made to accurately predict its occurrence. This prediction can be made few hours before it eventually emerges but there is possibility that there may be changes in the course of this hazardous event, which can undermine the accuracy of our forecasting.

3.1.3. **Vulnerability**

There are several factors responsible for any community's vulnerability to hurricane, and these include:

i. Location of the community: Those communities located in the low lying coastal areas are most susceptible to experiencing the direct of impact of hurricane. Again, those communities that are on the adjacent areas are also vulnerable to this hazardous situation. They often experience heavy rains and floods;

ii. Lack of risk education;

iii. Absence of adequate and effective warning systems;

iv. Lack of evacuation plans; and

v. Culture of poor erection of buildings or structures can also make any community vulnerable to hazardous events including hurricane. If the buildings and other physical structures in a community that experiences hurricane are constructed in a way non-resistant to hurricane damage, there is the tendency that building collapse will occur. These collapsed buildings and structures can result in huge losses in human and material terms;

3.1.4 **Risk reduction and preparedness measures**

i. Hazard mapping can be very useful in reducing the losses that hurricane may attract in any community. This is because hazards that are peculiar to any community may be identified and actions such as erection of buildings with no solid foundation can be avoided to reduce the damage that may be occasioned by hurricane or any other hazard;

ii. Upgrading of vegetation cover;

iii.   Land use control and flood management (see UNDP & UNDRO, 1992: 38);

iv.   Adequate evacuation plans and risk education;

v.   Effective public warning systems; and

vi.   Creation of community awareness and education on hazards and hazard mitigation can also help to reduce the effect of hurricane and any other hazardous events on any community.

3.1.5. **Impact assessment techniques**

The impact assessment of hurricane can be conducted through the use of damage assessment forms as well as aerial surveys

3.1.6. **Individual safety measures**

i.   If you are in a new place, you should seek information about the location of official shelters in time of hazardous incidents before hand;

ii.   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;

iii.   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;

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

v.   You should also equip yourself with transistor or battery radio, so that when there is an 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;

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

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

viii.   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

ix.   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.

x.   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 for recovery from the hazardous incident;

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

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

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

SELF ASSESSMENT EXERCISE

Discuss hurricane as a climatic security threat.

3.2   **Analysing Flood as a Climatic Hazard/Threat**

Flood is another climatic type of natural threat. It usually involves submerging of land by overflowing water. The meaning of flood goes beyond having volume of water like a river or lake that runs 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 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).

There are several types of flood, and they include

i.   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 can 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 the canal and putting-up a building structure on water passage, obstructing water-flow and the situation results in flooding. 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);

  ii.   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;

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

 iv.   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.

3.1.1 Effects of Floods

  i.   Destruction of infrastructure and other physical structures: Floods are capable of causing destruction. Effects of Floods particularly the severe one can destroy houses, sewer systems, bridges, schools, to mention a few;

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

iii.   Shortage of water: As a result of contamination of water, there may be (acute) shortage of drinkable water;

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

  v.   Outbreak of disease(s): The event of flood can generate an outbreak of diseases in the affected community. For instance, there is the possibility that where flood destroyed sewer system residents will experience water-borne diseases like cholera.

3.1.2 **Predictability**

The incidence of flood is predictable but in the case of storm surge or flash flood or tsunami, very little time (a few minutes) is given between when they become noticeable and their eventual occurrence. Notwithstanding, flood can be predicted with the use of various applications or approaches, which include flood forecasting based on seasonal patterns; flood plain mapping; capacity of drainage etc.

3.1.3. **Vulnerability**

i.   Areas located on floodplains;

ii.   Lack of risk education;

iii. Poor evacuation plans;

iv.   Lack of effective public warning systems; and

v.   Decrease in absorptive capacity of land especially through erosion;

3.1.4 **Risk reduction and preparedness measures**

i.   Flood control and floodplain management;

ii.   Well regulated building codes and ethics;

iii. Risk education and hazard mapping;

iv.   Adequate and effective evacuation plans; and

v.   Provision of effective public warning and alert systems;

3.1.5. **Impact assessment techniques**

Damage surveys forms and aerial surveys.

3.1.6. **Individual safety measures**

i.   If you know that you are staying in flood-ridden 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;

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

iii.   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, will know that it is important to have protective equipment (like life jacket, first-aid kits, etc) at home;

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

v.   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 the gadgets and electrical appliances, or even turn-off the power source (switch box);

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

vii.   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;

viii.   Ensure that you and other people in your household wear cover shoes to avoid infection like rashes;

ix.   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;

x.   Avoid using any electrical appliance enmeshed in water until technicians have instructed that they can be powered and used;

xi.   Always stay glued to your radio to get updates on the incident of flood;

SELF ASSESSMENT EXERCISE

How do you analyse flood as a climatic hazard?

3.3   **Analysing Drought as Climatic Hazard/Threat**

Drought is actually a normal climatic situation. It is experienced almost in all parts of the world. But, it can constitute a security threat if its occurrence is so significant. This is because it is supposed to be a temporary condition, which may last for sometime but its presence should not be too long. Drought appears to be another hazard that can lead to disaster if its effects are not mitigated by the people or the 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, definition of 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   . It can have a substantial impact on the   and   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 incidence of drought can lead to disaster except adequate interventionist measures and mitigation initiatives are brought into bear.

There is no doubt that the incidence of drought exists everywhere, particularly where there is high use of water. And this hazard has the potentials of undermining 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. However, there are various types of drought, which include the following:

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

ii.   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

iii. Hydrological droughts: These droughts 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.

3.1.1 Effects of Droughts

i.   Poor agricultural yields and crop production which can lead to food insecurity. 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;

ii.   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 the 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 not surprising, in the *Akaluka* religious riot in Kano, 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;

iii. Famine: Droughts can also generate famine due to lack of water for irrigation;

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

v.   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 a 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.

3.1.2 **Predictability**

Drought can also be predicted. Though, it is normal to experience some dryness in weather as associated with all world weather systems. But, significant dryness in weather can constitute a drought. However, we can predict the occurrence of drought through the analysis of rainfall and hydrology information about any community to determine if it is susceptible to experience future droughts.

3.1.3. **Vulnerability**

Any community can be vulnerable to drought resulting from the following factors:

   i.   Their location in an arid area;

   ii.   The attitude of cultivating on marginal lands;

   iii. Absence of agricultural inputs that can help to improve farm yields;

   iv.   Absence of seed reserves;

   v.   Lack of risk education and hazard mapping;

   vi.   Lack of early warning systems; and

   vii. Absolute dependence on other weather systems for water resources.

3.1.4 **Risk reduction and preparedness measures**

   i.   Drought and famine early warning systems;
   ii.   Land use control;

   iii. Development of inter-institutional response plan (see UNDP & UNDRO, 1992: 40); and

   iv.   Provision of risk education and promotion of community awareness of hazard mitigation and drought management.

3.1.5. **Impact assessment techniques**

Rainfall and hydrological data monitoring, socio-economic surveys, satellite imagery, among other tools can be used to assess the impact of drought on any community.

3.1.6. **Individual safety measures**

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

ii. 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;

iii. In various homes and offices, the culture of water management should be promoted. The use of toilets to urinate 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;

iv.   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;

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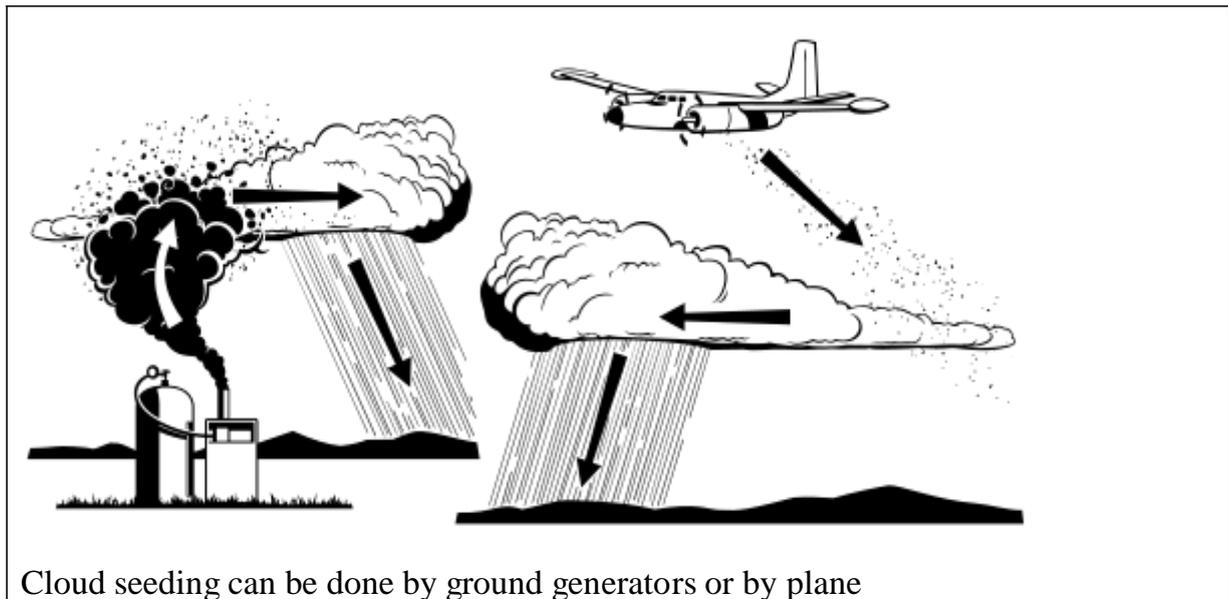
Source: ://upload.wikimedia.org/wikipedia/commons/thumb/4/4c/Cloud_ Seeding .svg/500px-Cloud_Seeding.svg.png.

SELF ASSESSMENT EXERCISE

How do you describe drought as a climatic security threat?

4.0   CONCLUSION

There is no doubt that if no adequate efforts are made to mitigate or reduce the impact of climatic hazards, there is the possibility that they will result in disasters. It is, therefore, important for stakeholders to adopt strategies through which they can improve their capacity to respond to these 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 has put in place measures and adopt 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 climatic types of security threat. We began our main task by looking at the meaning of hurricane as one of the climatic hazards or threat and

analysed how it constitutes a security threat to any community. Thereafter, we drew our analytical searchlight on the second type of climatic security threat or hazard, flood, and we explained how it poses a huge risk to communities or people. The last type of climatic hazard we discussed in this unit was drought. In our analysis of drought as a climatic hazard, we explained its meaning and other issues including its effects and predictability, among others. I have no doubt that you have found this unit thought-provoking.

6.0   TUTOR-MARKED ASSIGNMENT

i.   Define three types of climatic hazard or threat; and
ii.   Enumerate any four factors that can make any community vulnerable to flood.

7.0   REFERENCES AND FURTHER READING

Albert, I.O. (1999). Ethnic and Religious Conflicts in Kano. 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.

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

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.

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.

://en.wikipedia.org/wiki/Drought. 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.

://upload.wikimedia.org/wikipedia/commons/thumb/4/4c/Cloud_Seeding.svg/500px-Cloud_Seeding.svg.png. Retrieved on 2 October, 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.

://www.semo.state.ny.us/info/publicsafety/hurricaneprepare.cfm. Retrieved on 30 August, 2009.

://www.vigyanprasar.gov.in/comcom/feature64.htm. 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 4

ANALYSIS OF ENVIRONMENTAL SECURITY THREATS I

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Body
        3.1   Desertification as an Environmental Security Threat
        3.2   Deforestation as an Environmental Security Threat
4.0   Conclusion

1.0.   INTRODUCTION

In the last three units, our focus had been centred on geological and climatic types of security threat. Those two sets of security threat types have been largely natural but we cannot rule out the possibility of man-made activities and actions as contributing to their occurrence. Unlike, geological and climatic threats or hazards, environmental threats have manmade cause even more than nature. The fact is that unfriendly handling of environmental resources by man has been the major factor responsible for the occurrence of various types of environmental security threats.

However, in this unit, we shall focus on environmental threats but due to limited space and time that we have in this unit, we shall study two of the four types of environmental threat that we have considered in this course for analytical inquiry. The two environmental threats that we shall beam our searchlight on in this unit are desertification and deforestation. Before we go into the nitty-gritty of this study, let us quickly browse through the various tasks that we shall be undertaking in this unit. The tasks are stated in the next segment of this unit (Objectives).

2.0   OBJECTIVES

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

• Identify desertification and deforestation as forms of environmental threats;

• Define desertification and analyse how it constitutes a security threat; and

• Describe and examine deforestation as an environmental threat.

3.0   MAIN BODY

3.1   Desertification as an Environmental Security Threat

Desertification is one of the major environmental threats. The contradictions it has mounted have posed very adverse effects on man and his/her environment. It is usually occasioned or caused by the absence or drastic reduction in the volume of rainfall such that rainfall dwindles below normal recorded levels for long period of time. Desertification is a major contributor of drought, capable of causing poor yield to agricultural production especially farming. It is worrisome that "seventy percent of the world's drylands (excluding hyper-arid deserts), or some 3,600 million hectares, are degraded" (://www.gdrc.org/uem/Trialogue/whatis-desert.html. If the situation is

not addressed, there is the possibility that more people will be in hunger and starvation. However, what is desertification? Desertification can be described as:

...the process by which productive or habitable land becomes gradually more arid and less capable of sustaining vegetation, eventually turning into desert. It is often a cause of long-term disasters (://www.ifrc.org/what/disasters/about/types/climatological/drought.asp).

..the progressive destruction or degradation of existing vegetative cover to form desert. This can occur due to overgrazing, deforestation, drought, and the burning of extensive areas. Once formed, deserts can only support a sparse range of vegetation... (.climatechange.ca.gov/glossary/letter_d.html).

...the degradation of drylands. It involves the loss of biological or economic productivity and complexity in croplands, pastures, and woodlands. It is due mainly to climate variability and unsustainable human activities. The most commonly cited forms of unsustainable land use are overcultivation, overgrazing, deforestation, and poor irrigation practices (://www.gdrc.org/uem/Trialogue/whatis-desert.html).

...the degradation of land in arid and dry sub-humid areas, resulting primarily from man-made activities and influenced by climatic variations. It is principally caused by overgrazing, overdrafting of groundwater and diversion of water from rivers for human consumption and industrial use, all of these processes fundamentally driven by overpopulation (://en.wikipedia.org/wiki/Desertification).

...the gradual transformation of habitable land into desert; is usually caused by climate change or by destructive use of the land (**Error! Hyperlink reference not valid.**).

3.1.1 Effects of Desertification

i.   Reducing the Capacity to produce Food: The incidence of desertification poses enormous challenges to any affected communities especially as it largely undermines the capacity of such communities to feed themselves, as they will to a large extent rely on other communities to meet the feeding needs of their population. Undoubtedly, this environmental security threat has become a major issue among the world population in recent time owing to the continued significant variability in the global climate. This is a result of the relationship between dryland degradation and climate change, provoking desertification on one hand and the link between desertification and drastic fall in the ability of any affected community to produce food culminating in starvation and nutritional inadequacy on the other hand.

The problem of desertification has been affecting quite a number of African countries including Niger and Chad. The ravaging hunger and starvation produced by the incidence of desertification in Africa has continued to

undermine its security, as the continent has been continually confronted with civil strife, ethno-religious violence, violent crimes especially armed robbery among other threats. More unfortunately, absence of good governance and creative leadership has further reinforced the agonies mounted by desertification in several parts of the continent. There is growing involvement of foreigners especially from neighbouring countries like Chad and Niger in armed robbery and many other violent crimes in northern Nigeria, which has resulted in huge losses in human and material terms;

ii.   Famine: Desertification often instigates problem of famine in the affected communities. This situation creates poverty among the mass public. There will be poor yields in food production such that food distribution will be hampered, and it is only those that can afford the exorbitant prices of the available food commodities that can have access to them (food).

Consequently, majority of the people will have to make hunger and starvation their second nature because of high cost of purchasing food, and many of whom may already be economically disarticulated resulting from some socio-economic factors (like unemployment, poor wages, seclusivism etc), as they will always be on the brink of explosion.

As you may agree with me, a hungry man will always exhibit attitudes of aggression. In a situation like this, one should not be surprised that the affected communities will have to cope with growing rate of violent crimes, social vices including prostitution, civil unrest, war or insurgency. In communities where acute food shortage exists, the security practitioners or law enforcement agents face a great challenge in maintaining law and order because the attendant crime rate may overwhelm their capacity to guarantee security of lives and property within their respective jurisdictions;

iii.   Forced migration: Desertification can threaten the lives of people due to extremely harsh conditions like the hunger it foists on them. Many of the affected people forcefully migrate to other places in search of greener pasture or where there is absence of food shortage (or mass hunger and starvation). For instance, there has been an exodus of Taureg from desertification-ridden Niger Republic, migrating to many Nigerian cities like Kano in search of better socio-economic wellbeing while many of them who are farmers have been forced to migrate seeking for fertile land where they can do their farming or cultivation.

But, the continued problem of desert encroachment being experienced in many parts of northern Nigeria has heightened the frustration of many of these migrant Taureg farmers. The hopes of a great number of them were dashed as they have found it difficult to secure land for cultivation, and for the lucky ones among them who have gained access to land for cultivation, drastic reduction in the volume of rainfall has greatly undermined the farm yields. The excruciating plague of unemployment in Nigeria has also deepened the

frustration of the migrant Tuareg as many of them have resolved to engage in criminal activities like armed robbery and religious violence;

iv.   Economic underdevelopment: Inability of any nation to feed its people sufficiently resulting from desertification or any other factors can lead to its (over)reliance on other countries for food, which will have a negative impact on its economy. The reason is that such affected nation will most likely resort to importing food and may be spending a large percent of its earnings on the importation of food, which it may even subsidise in order to make food affordable to the people. According to a source, the amount of financial resources depleted by desertification is mammoth and thus globally:

> *...it is estimated that the annual income foregone in the areas immediately affected by desertification amounts to approximately US$ 42 billion each year. The indirect economic and social costs suffered outside the affected areas, including the influx of "environmental refugees" and losses to national food production, may be much greater* ([://www.gdrc.org/uem/ Trialogue/whatis-desert.html](://www.gdrc.org/uem/Trialogue/whatis-desert.html); and
.

v.   Environmental scarcity: Dryland degradation can attract environmental scarcity whereby the affected community experiences drastic reduction in harvest. Farming activities will record very little or no yields as a result of desertification leading to environmental scarcity. The environmental scarcity is also capable of creating tension and engendering violent crime as may be reinforced by poor food distribution and injustice in the sharing of state resources like land allocation.

3.1.2 **Predictability**

Desertification as an environmental security threat can be predicted. In carrying out surveillance of drylands to determine the amount of desertification that occurs in any particular community, we can use remote sensing and/or aerial surveys.

3.1.3. **Vulnerability**

There are several factors that are responsible for vulnerability of any community to the incidence of desertification, and these include:

i. Experience of low rainfall and high temperatures;

ii. Uncontrolled and heavy land use;

iii. Absence of effective irrigation management;

iv. Application of inappropriate agricultural technologies and mundane cultural farming techniques; and

v. Mass poverty and overpopulation;

3.1.4 **Risk reduction and preparedness measures**

i. Establishment of policies and laws that can promote sustainable agricultural development, which can reduce the problem of desertification;

ii. Creating awareness and education to the people on the ways that they can mitigate the problem of desertification;

iii. Promotion of hazard mapping and risk education among the people to enable them identify those actions or activities that propel desertification and appreciate the level of threat posed by desertification to them individually and collectively. This will definitely make them to be more prepared towards reducing the losses that such hazardous situation can bring on them and their community at large;

iv. Developing strategies to improve soil quality especially through effective land control; and

v. Stepping-up of desertification monitoring and conducting on regular basis the available monitoring systems and mitigation approaches are also essential to reducing vulnerability.

3.1.5. **Impact assessment techniques**

Aerial and remote sensing surveys are very germane in measuring the rate and scope of desertification. Again, we can also use socio-economic surveys to determine the needs of people in agricultural planning and sustainable agricultural development (see UNDP & UNDRO, 1992: 43).

3.1.6. **Individual safety measures**

i. Ensure you absolutely discourage any water wastages;

ii. Cutting down of trees should be drastically reduced;

iii. There should be effective irrigation measures to mitigate the effect of desertification;

iv. There should be conservation of soil, and we should avoid using any land too much for cultivation; and

v. It is helpful to get awareness and education on appropriate agricultural technologies and activities that reduce the effect of desertification.

SELF ASSESSMENT EXERCISE

How will you describe desertification as a form of environmental threat?

3.2   **Analysing Deforestation as an Environmental Threat**

Deforestation is another type of environmental threat. It usually involves felling or burning of trees by human beings for different purposes that may include using trees as firewood for cooking, converting the forest into agricultural site or residential location. The reckless felling of trees poses a great security risk to any community. It has a very serious impact on the habitat, biodiversity and even aridity. Generally, deforestation adversely affects the biosequestration of atmospheric carbon dioxide, posing a huge threat to man and his/her environment. At this point, let us browse through some of the available definitions of deforestation. Thus, deforestation can be described as:

...those practices or processes that result in the change of forested lands to non-forest uses. This is often cited as one of the major causes of the enhanced greenhouse effect for two reasons: 1) the burning or decomposition of the wood releases carbon dioxide; and 2) trees that once removed (.climatechange.ca.gov/glossary /letter_d.html)

...destruction of forests to make land for agriculture. Cutting down trees, which provide oxygen and absorb carbon dioxide, is seen as a cause of increased greenhouse effect. Deforestation also entails the destruction of animal habitats (_. learn-english-today.com/environment/env-vocabulary.html).

...the clearance of naturally occurring forests by the processes of logging and/or burning of trees in a forested area. There are several reasons deforestation occurs: trees or derived charcoal can be sold as a commodity and used by humans, while cleared land is used as pasture, plantations of commodities and human settlement (://en.wikipedia.org/wiki/Deforestation).

Evidently, deforestation often attracts soil erosion, causing ecological quandary in the midst of unfavourable socio-economic conditions. Globally, the incidence of deforestation has been on the increase as it has been estimated that almost half of the world's mature tropical forests has been defiled through reckless removal of trees (see Nielsen, 2006). In Nigeria, the problem of deforestation has been endemic as several parts of the nation continue to battle with harsh ecological conditions that deforestation has mounted. For instance in Kano, the growing depletion of forests has been worrisome. According to Eckholm *et al*. (1984):

over the last 25 years, commercial wood demands have led to severe deforestation and the collapse of a sustainable agricultural system ... now farmland within a 40 km radius of the city (of Kano) has been largely stripped of trees (Eckholm *et al.*, 1984: 28) .

It is more worrisome that despite the adverse effects of deforestation, people have continued to remove trees with little or no concern about replacing them with new ones. The culture of using trees as firewood for cooking has contributed largely to the depletion of forests in Nigeria especially as Kerosene is almost out of reach of the downtrodden. Considering the consequences of deforestation, one will not but agree that deforestation pose a huge security threat to man. We shall explain these adverse effects in the next part of the segment.

3.2.1 **Effects of Deforestation**

i. Adverse Atmospheric Conditions: It is popularly accepted that deforestation contributes significantly to climate change as it has remained one of the leading contributing factors of the enhanced greenhouse effect. Tropical deforestation is believed to account for almost 20% of global greenhouse gas emissions (://www.fondationchirac.eu/en/deforestation). Among anthropogenic activities that aid the emission of carbon dioxide into the atmosphere, deforestation accounts for almost one-third (://www.ipcc.ch/pdf/assessm ent-report/ar4/wg1/ar4-wg1-chapter7.pdf).

Usually, trees and other plants through the process of photosynthesis assist the atmosphere to remove carbon dioxide that destroys the atmosphere by returning oxygen into the atmosphere during normal respiration (**Error! Hyperlink reference not valid.**). But by burning down the forest or trees, we are trapping the atmosphere with Carbon dioxide, which damages the atmosphere. Again, by removing trees, we reduce the amount of oxygen produced by the trees to the atmosphere, and this oxygen helps to maintain its good quality and biosphere stability;

ii. Poor hydrological conditions: Water is very vital to the wellbeing of any people or community, and so forestation is important to water cycle. There is no doubt that deforestation also contributes in no small measure to distortion in the water cycle. Trees through their roots help in extracting groundwater, which it releases to the atmosphere for the atmosphere to maintain its biosphere stability. Thus, reckless removal of trees rapidly reduces the amount of groundwater emitted into the atmosphere by trees, and the consequence of this action (deforestation) is invocation of much drier climate;

iii. Loss of Soil Cohesion or erosion: Another adverse effect that deforestation poses to any community or people is loss of soil. The reason is that deforestation contributes in no small measure to soil erosion as it increases the quantity of runoff and cuts down the protection that tree litter gives to soil. It is

worrisome the rate at which soil loss is engineered resulting from deforestation, and it is believed that "approximately 2 metric tons per square kilometre" of soil are lost due to rapid decimation of forest or deforestation (://en.wikipedia.org/wiki /Deforestation). Trees through their roots help to encourage soil cohesion especially when the soil appears to be shallow, the trees "act to keep the soil in place by also binding with underlying bedrock" (ibid). Deforestation can therefore lead to the loss of soil cohesion and where we have shallow soil, the risk of landslides becomes more imminent;

iv.   Ecological Hazard: Deforestation is also known to be one of the leading contributors of decline in biodiversity (://www.actionbioscience.org/ environment/nilsson.html). Forestation helps to sustain biodiversity, as it provides habitat for wildlife. Since tropical rainforests accommodate almost 80% of the world's biodiversity, decimation of trees can propel a rapid reduction of biodiversity with attendant consequence of environmental degradation.

Again, apart from the animals that are harboured in the forests some of which may go into extinction resulting from deforestation (loss of habitat) and hunting, the medicinal conservation being engineered by forests will become diminished such that some plant species may be wiped-out. This situation can also have a very negative effect on the wellbeing of man and his/her environment; and

v.   Economic Underdevelopment: Massive removal of trees or depletion of forests can drastically reduce the living standards of communities as it has been argued that if care is not taken deforestation will propel a reduction of global GDP by almost 7% by year 2050 (see ://en.wikipedia.org/wiki/Defore station).

3.2.2 Predictability

Hazard mapping and global attention has increased with a view to mitigate the problem of deforestation. Thus, deforestation is predictable, and due to growing awareness concerning the threat posed to global population by deforestation, more information is emerging about those activities that promote the problem of deforestation. The information has made it easy to identify the rate and scope of deforestation that takes place in any community.

3.2.3. Vulnerability

i. Population explosion: A rapid growth in the population of any community is one of the factors contributing to the vulnerability of such community to the problem of deforestation. One of the reasons is that there will be an increase in the demand for wood for different purposes including furniture;

ii. Rapid urbanisation: A situation whereby a community is rapidly urbanising, there is tendency that there will be growing depletion of forests especially by converting many of the forests to residential quarters as being experienced in many of the cities in Nigeria including Kano and Lagos;

iii. Mass poverty: Where there is endemic poverty among the larger segment of the society, there is tendency that such a society will become more vulnerable to deforestation. Many of the people who cannot afford kerosene and cooking gas for their cooking often resort to using trees as firewood;

iv. Unregulated removal of trees: Any community can become much more vulnerable if people recklessly cut-down trees without any attempt to replace the lost trees through re-plantation of trees or reforestation; and

v. Economic dependence on wood: In communities where many rely solely on wood for income, deforestation is widely carried-out with very severe consequences on the economy of those communities. For instance, exportation of timber by many West African countries has really hampered the capacity of many of these countries to meet their local demand for timber with attendant adverse impact on their furniture industry. Thus, many of them have ended up importing furniture abroad to address shortage in furniture production on the home-front. This situation will therefore have more negative impact on their national economies.

3.2.4 Risk reduction and preparedness measures

i. Conservation of forests can be encouraged to reduce the incidence of deforestation;

ii. Necessary legislations or laws should be formulated and adequately implemented to discourage those actions and activities that promote rapid removal of trees or deforestation;

iii. Provision of social amenities in rural areas can also reduce the influx of migrants to urban centres. By doing so, there will be drastic reduction in accommodation requests in the cities which can propel conversion of forests into residential sites for the yearning urban residents;

iv. Hazard mapping is also vital in mitigating the problem of deforestation. Through hazard mapping, we may be able to identify the rate at which in all locations or areas trees are being decimated for prompt mitigation response;

v. As you may know, population explosion is one of the causes of deforestation, it is therefore important to educate the masses on the relevance of birth control in preserving their environment and reducing the problem of deforestation; and

vi. The government should also make kerosene and cooking gas available and very affordable to people such that the use of firewood for cooking will become less attractive to them especially the downtrodden.

3.2.5. Impact assessment techniques

We can map the rate and scope of deforestation by using aerial or remote sensing or ground surveys.

3.2.6. Individual safety measures

i. We should cultivate the habit of planting trees on regular basis;

ii. The cutting down of trees for firewood to do our cooking should be avoided. Instead, we should use either kerosene or cooking gas. Though, many people may argue that they cannot afford kerosene or cooking gas but the one fact that we cannot do away with is that the consequences of deforestation are very severe, and the poor usually appear to be the most vulnerable.

For instance, where flooding is experienced resulting from deforestation, and in worst-case scenario whereby massive structural and physical damage is recorded like the collapse of buildings, it is the poor that suffer more because they may not afford any alternative accommodation if their houses are badly damaged. It is against this background that we should also educate the downtrodden to take the issue of reforestation more seriously and avoid actions that promote the problem of deforestation;

iii. There should be use of bricks instead of wood in the construction of buildings or shelter;

iv. We should educate our household on the need to avoid reckless removal of trees; and

v. We should avoid engaging in bush-burning, which apart from contributing to deforestation can also entrap the atmosphere with carbon dioxide (CO_2) that propels climate change, capable of causing some other hazards like drought and desertification.

SELF ASSESSMENT EXERCISE

Discuss deforestation as an environmental threat.

4.0   CONCLUSION

Considering some facts that have emerged about our analysis of desertification and deforestation, you may agree with me that these environmental threats are highly preventable, provided that every people and community can pay greater attention to conservation of environmental resources as well as providing effective mitigation strategies to rapidly reduce any losses that occurrence of these threats can pose them. It is worthy to note that these environmental threats have the capability of leading to another set of threat types. For instance, deforestation can generate drought (a climatic threat), capable of shortening or reducing the capacity of any community to feed itself especially as a result of drastic reduction in the volume of rainfall or levels of water. It is therefore important for all stakeholders to take environmental issues more seriously especially through development of viable framework through which these environmental threats can be mitigated.

5.0   SUMMARY

In this unit, we have been able to discuss two environmental threats (desertification and deforestation). We began by explaining the meaning of desertification and subjected it to analytical scrutiny in exploring how it constitutes a threat to any people or community if it occurs. We also focused on other relevant issues that bother on its predictability, what factors are responsible for vulnerability of community etc. Thereafter, we analysed deforestation as another form of environmental threat by defining it, explaining its predictability among other issues relevant to the subject.

6.0   TUTOR-MARKED ASSIGNMENT

i.   Define deforestation and desertification; and

ii. Briefly discuss any three mitigation measures to each of these two environmental threats.

7.0   REFERENCES AND FURTHER READING

Eckholm, E., Foley, G., Barnard, G. and Timberlake, L. 1984. *Firewood: the energy crisis that won't go away*. Earthscan (IIED).

Nielsen, R. (2006). *The Little Green Handbook: Seven Trends Shaping the Future of Our Planet*. New York: Picador.

UNDP & UNDRO (1992). *An Overview of Disaster Management* (2nd Edition). Disaster Management Training Programme.

://en.wikipedia.org/wiki/Desertification. Retrieved on the 15 October, 2009.

://www.actionbioscience.org/environment/nilsson.html. Retrieved on 30 October, 2009.

://www.fondationchirac.eu/en/deforestation. Retrieved on the 15 October, 2009.

://www.gdrc.org/uem/Trialogue/whatis-desert.html. Retrieved on the 6 September, 2009.

://www.ifrc.org/what/disasters/about/types/climatological/drought.asp. Retrieved on 9 October, 2009.

://www.ipcc.ch/pdf/assessment-report/ar4/wg1/ar4-wg1-chapter7.pdf. Retrieved on 20 October, 2009.

.climatechange.ca.gov/glossary/letter_d.html. Retrieved on 10th October, 2009.

. learn-english-today.com/environment/env-vocabulary.html. Retrieved on 10 October, 2009.

.wordnetweb.princeton.edu/perl/webwn. Retrieved on 10 October, 2009.

UNIT 5

ANALYSIS OF ENVIRONMENTAL SECURITY THREATS II

CONTENTS

1.0.   INTRODUCTION

In the last unit, our focus was centred on two forms of environmental security threat including desertification and deforestation but in this unit we shall conclude our tasks on the types of environmental threat by examining the last two types of environmental threat. These include environmental pollution and pest infestation. These environmental threats like the other two already discussed in the last unit, can also pose enormous challenge and a huge threat to people or communities. Environmental pollution apart from mounting a huge threat on its own to any people can also generate some other hazards like drought, climate change and flood that may also pose greater security risk to the survival of communities or people.

On the other hand, apart from the threat posed by pest infestation to crops and human beings, it can also undermine the economic survival of people, and is capable of mounting on any affected people environmental scarcity that can exacerbate existing socio-economic tension. At this point, let us take a glimpse at the various tasks that we will accomplish in this unit. These tasks are enumerated in the following segment of this unit.

2.0   OBJECTIVES

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

- Explain the meaning of environmental pollution, and analyse how it can constitute a threat to people or communities; and

- Describe pest infestation as an environmental form of security threat.

3.0   MAIN BODY

3.1   Analysing Environmental Pollution as a Security Threat

Environmental pollution is usually experienced when those contaminations or anthropogenic blotting of the environment cannot be sufficiently processed and neutralised by the environment "without any structural or functional damage to its system" (://www.tropical-rainforest-animals.com/Environmental-Pollution.html). It is no surprise that environmental pollution is often regarded by many people as silent killer. People always engage in activities that pollute the environment such as a emission of gases into the atmosphere, trapping the atmosphere with carbon dioxide that usually attracts significant variability in climate.

124

Sometimes, people pollute their environment ignorantly especially through some cultural practices. For instance, in some communities burning down of forests for cultivation has become a normal practice without considering the amount of damage it can pose their environment. Apart from increasing the problem of climate change, it can also lead to some other hazards like flood and drought among others. However, at this point, it is important to explore some of the common definitions of the term, environmental pollution. As you may be aware, the list of definitions of environmental pollution is long, but we can define it:

...the introduction of contaminants into an environment that causes instability, disorder, harm or discomfort to the ecosystem (://en.wikipedia.org/wiki/ Environmental_pollution).

...contamination of air, water and land from man-made waste. Pollution leads to depletion of the ozone layer, global warming and climate change. Air pollution is the release of chemicals and particles into the atmosphere. Water pollution includes surface runoff, leakage into groundwater, liquid spills, wastewater discharge and littering. If toxins are spilled on the ground or if an underground storage tank leaks, soil can become contaminated. Well known contaminants include herbicides and pesticides. Toxic waste is waste material, often in chemical form, which pollutes the natural environment and contaminates groundwater (**Error! Hyperlink reference not valid.**).

...the contamination of the physical and biological components of the earth/atmosphere system to such an extent that normal environmental processes are adversely affected (Kemp, 1998: 129).

...the addition of any substance or form of energy (e.g., heat, sound, radioactivity) to the environment at a rate faster than the environment can accommodate it by dispersion, breakdown, recycling, or storage in some harmless form (://library.eb.co.uk/eb/article-9109632).

...any use of natural resources at a rate higher than nature's capacity to restore itself can result in pollution of air, water, and land (Santos, 1990: 44).

Considering the above definitions, there are various forms of environmental pollution, and they can be basically classified as air pollution, water pollution and soil contamination. There is no doubt that the consequences of environmental pollution can be so severe not only man but also to the general ecosystem. Meanwhile, the adverse effects of pollution are many but in this unit, we shall explain some of them. This task shall be undertaken in the next part of this segment of the unit.

3.1.1 **Effects of Environmental Pollution**

i.   Health risk: Environmental pollution can pose a great security risk to public health. This is because it has the capacity to cause reduction in lung

functioning, increase in cases of asthma attacks, respiratory disorder especially in the form of coughing and wheezing, growing rate of disruption of endocrine, reproductive and immune systems. It can also contribute to a drastic increase in some other health problems like cancer; cardiovascular disorder; irritation of eyes, nose, mouth and throat; as well as premature death.

For instance, through pollution of water, people can get cholera, typhoid, hookworm etc. It is therefore very important for one to treat his/her water before drinking. Even, if one wants to use water for bath, it is germane to treat it with the use of disinfectants. The truth is that many people often get infected with rashes, ear ache, hepatitis, gastroenteritis, diarrhea etc when they bathe themselves with some contaminated water (://www.tropical-rainforest-animals.com/Environ mental-Pollution.html). In situations where there is contamination of water through some chemicals like hydrocarbon and pesticide, there is the possibility that a number of people will be inflicted with cancer, liver and kidney damage etc;

ii.   Destruction of crops and aquatic systems: Environmental pollution can cause contamination of air and atmosphere, which can result to destruction of agricultural crops and forests. It can also lead to the destruction of aquatic systems. For instance, through the emission of greenhouse gases, we trap the atmosphere with carbon dioxide (CO_2), which can provoke a rapid variability in climate (climate change). Climate change can on its own mount a situation whereby there will be drastic reduction in the volume of rainfall, which can also lead to increasing reduction in the level of water in the river or sea;

iii. Spread of pathogens and toxins: The pollution of water can reduce water quality with attendant risk to the health of the people and sealife. There is no doubt that the problem of growing environmental pollution in the Niger Delta region of Nigeria has really affected sealife in this area. The effluents and pollutants generated by oil exploration and some other industrial activities have damaged the aquatic systems in this area such that fishing has become a non-vibrant venture;

iv.   Environmental scarcity: Pollution can lead to acute shortage of food, livestock and water resources including fishes. For instance, the contamination of farm lands can propel loss of farm yields or destruction of crops, which can undermine the capacity of any community in the production of food. Pollution can also produce acid rain, which can kill trees and damage the leaves of plants as well as drastically reducing the quality of soil, losing its potentials to produce nutrients to plants; and

v.   Global warming: Environmental pollution has an adverse effect on the atmosphere. It can attract a rapid rise in the temperature in the affected community. It can also contribute to sea rise and climate change (see UNDP & UNDRO, 1992: 41).

3.1.2 **Predictability**

Environmental pollution is a subject of per capita consumption. Through development of any country or community, we can predict the susceptibility of such country or community to the incidence of environmental pollution.

3.1.3. **Vulnerability**

i.   Rapidly growing rate of industrialisation is one of the factors that determine the vulnerability of any community to the problem of environmental pollution. High industrialisation is capable of subjecting the environment to all forms of pollution. The effluence and the huge amount of gas emissions produced by several industrial activities often damage ecosystem and undermine the public health of people or community especially when there are no adequate laws to regulate how these industries dispose and manage their wastes;

ii.   Absence of pollution control regulations can make any community vulnerable to pollution because people or industries engage in all sorts of actions that promote environmental pollution with impunity. If there are laws guiding people on how they dispose their wastes, the anthropogenic activities can be minimised if not curbed totally;

iii. Lack of mitigation plans and risk education can also complicate the problem of pollution in any community. The reason is that most people or industries will not know the amount of risk that various pollutions can pose to the general wellbeing of their environment if there is absence of risk education. Also, if there are no adequate mitigation plans, people will not be able to identify those action that they can undertake to reduce the effect of pollution on their lives and environment; and

iv.   Another factor that can make any community vulnerable to pollution is widespread poverty or unequal distribution of state resources. Due to the inability of many people in most developing countries to afford modern farm mechanisation, many farmers still engage in old cultivation practices like bush burning as they increase the amount of carbon dioxide that is emitted into the atmosphere. In sub-Saharan Africa, there still exist several homes without toilets whereby people urinate and excrete their body wastes into the rivers, from where people will still go and fetch water for domestic use with very severe consequences to public health.

3.1.4 **Risk reduction and preparedness measures**

i.   Establishment of laws to control all forms of pollution;

ii.   Risk education and mitigation plans;

iii.   Drastic reduction in the use of pesticide;

iv.   Hazard mapping is also essential to mitigate the problem of environmental pollution especially by identifying the level and scope of pollutions in each part of the community;

v.   There should be effective control of the use of aerosol and disposal of refrigerators (see UNDP & UNDRO, 1992: 41);

vi.   Invocation of initiatives that promote reforestation and drastic reduction in the incidence of deforestation; and

vii.   The production and use of chlorofluorocarbons (CFCs) should be discouraged because of its potential in generating depletion of the ozone layers.

3.1.5. **Impact assessment techniques**

According to UNDP & UNDRO (1992: 41), the techniques through which we can assess the impact of environmental pollution in any area or community may include:

i.   Aerial, remote sensing and ground surveys;

ii.   Application of air, water and soil testing to determine the level and scope of pollution in the affected area;

iii.   Comparative study of climatic data; and

iv.   Socio-economic surveys can also be useful to determine the level of economic vulnerability of the people, how much do poor socio-economic conditions exacerbate the problem of environmental pollution, and how much impact does environmental pollution have on the socio-economic condition of the community at large.

3.1.6. **Individual safety measures**

i.   Avoid dropping wastes into the canal;

ii.   Educate your household on the need to avoid engaging in activities that can promote emission of greenhouse gases into the atmosphere especially bush burning or burning of refuse;

iii.   Report any individual or organisation engaging in destroying the sealife by disposing effluents and pollutants into the sea or river or stream;

iv.   Avoid defecating in public places and ensure that toilets are available in your houses. It is also important to report any house without toilet(s) to sanitary authorities for appropriate punishment; and

v.   Reckless removal of trees from forests should be discouraged in strong terms etc.

SELF ASSESSMENT EXERCISE

Analyse environmental pollution as a security threat.

3.2   **Analysing Pest Infestation as a Security Threat**

Pest infestation can pose a huge security risk to any community owing to the rate at which it can potentially undermine the capacity of the community to produce food. A source has argued that due to pest infestation:

It is estimated that 35% of world crop production is lost in spite of pesticide and other control programs. The primary pests are insects, disease and weeds. Losses due to birds and wild animals are low compared to these ([://nidm.gov.in/Pest_ Infestation.asp](://nidm.gov.in/Pest_Infestation.asp)).

Considering the foregoing, infestation is basically caused by such pests like insects while some animals can also pose a great danger to a community. On farmlands, we may also have human pests who usually keep a close watch on farmers with criminal intent, to cart away the harvests and deprive the farmers the opportunity to enjoy the fruits of their labour.

Generally, insects and animals as pests pose a huge threat to a community, as we cannot also rule-out the potentials of ants and earwigs to cause people severe damage with very adverse impact on their public health and material resources. Conceptually, for the sake of clarity, we shall attempt the definition of the term by separating the two words (pest and infestation) that it consists. First, we shall be considering the meaning of pest. Thus, pest can be defined as:

...as any living organism or plant causing harm or damage to people, their animals, crops or possessions. The important pests are those, which lead to loss of crop yield or quality, resulting in loss of profits to the farmers and reduced stocks for subsistence or export ([://nidm.gov.in/Pest_ Infestation.asp](://nidm.gov.in/Pest_Infestation.asp)).

On the other hand, infestation can simply be defined as:

...the act of infesting or to overrun or haunt in large numbers, especially as to render unpleasant or unsafe (Funk & Wagnalls Standard Dictionary, 1962).

However, if we merge the two definitions above, we cannot be wrong to define pest infestation as (destructive) overrunning or haunting of people, animals, crops or possessions by any living organisms especially insects with the capacity to pose a huge risk to the affected and undermine their safety and security. Another definition of pest infestation is that it is:

...the occurrence of one or more pest species in an area or location where their numbers and impact are currently or potentially at intolerable levels (**Error! Hyperlink reference not valid.**).

There is no doubt that pest infestation can undermine the food production capacity of a community because it can drastically reduce farm yields by destroying the plants' stems and root systems as well as infuse toxins on the farmlands (UNDP & UNDRO, 1992: 44). A number of ecological factors contribute to the incidence of pest infestation, and one of them is temperature. Temperature has become the chief contributor to pest infestation. One reason is that hot temperature assists the pests to develop and replicate much rapidly. Other factors may include mono-culture of crops; migration, introduction of new plants to new locations, among others. The negative impact that pest infestation may have on a community can be so severe owing to the various adverse effects it manifests when it occurs in any area. We shall explain these effects in the next part of this segment.

3.2.1 Effects of Environmental Pollution

i.   Propelling damage of crops: Pests may destroy plants or crops especially by attacking their roots resulting in poor agricultural yields and loss of profits for the farmers;

ii. Food insecurity: The poor yields on agricultural activities as mounted by pest infestation can reduce the potential of any affected community in food production. Nonetheless, pest infestation has been identified as one of the leading contributors of famine capable of subjecting people to ravaging hunger and starvation;

iii. Economic underdevelopment: Due to wide destruction of crops, the capacity of any affected community to reserve crops for export will rapidly diminish, meaning that a lot of foreign earnings will be lost in the process;

iv.   Poverty: Pest infestation generates poverty especially among agricultural practitioners who lose the larger parts of their productions to pests. Through pest infestation, many agricultural workers may record high profit loss, making them economically vulnerable; and

v.   Health Hazard: Pest infestation can also cause a health hazard to any people or communities. For instance, there is increasing risk of lassa fever where there exists Natal Multimammate Mouse (Mastomys natalensis). This disease is usually caused by some rodents popularly called lassa rats by defecating and

urinating on grains and other food items as well as kitchen utensils. Any human being that comes in contact with such feces or urine either by eating the infected grains or food items or using any kitchen utensils without being treated may be infected with lassa fever (an acute viral hemorrhagic fever). This disease is very fatal as it can result in many deaths in the affected communities.

3.2.2 Predictability

Pest infestation is highly predictable as the use of pest forecasting can be so helpful not only in detecting the level and scope of infestation but also in identifying the types of pesticide that can be cost effective in mitigating the infestation. Proper monitoring of crops and/or livestock can also assist us to detect and determine the types and amount of pests that exist, which can cause damage to our crops and/or livestock.

3.2.3. Vulnerability

There are several factors that can make communities vulnerable to pest infestation, and these include:

i.   Existence of large number and variety of pests;

ii.   Existence of high temperature can foster a rapid development of pests;

iii. Poor sanitary conditions can also assist the pests to replicate so fast because they usually have access to food and other wastes not well disposed. They feed on these wastes and become multiplied. For instance, rats will always visit places where they can easily have access to food;

iv.   Absence of adequate pest control which can make a community vulnerable; and

v.   Absence of advanced agricultural technologies.

3.2.4 Risk reduction and preparedness measures

i.   Application of appropriate and effective pest control measures can be helpful in reducing the incidence of pest attacks or damage. It is also important to examine the side effects of every pesticide in order to enhance public safety;

ii.   Cleanliness is usually regarded as next to godliness. It is very germane to clean our environment with the aim of controlling the pests;

iii. Pest identification is also essential in reducing the impact of pests on any area or community. By identifying types of pest available in an area, we can determine the level and scope of the infestation as well as forms of pesticide that can be applied to rapidly reduce their damage;

iv.   Risk education is also vital to create awareness among the people on those factors that aid pest infestation and how they can be addressed. This may enable them to act more creatively and effectively in reducing the losses that pest infestation can inflict on them; and

v.   Existence of integrated pest management is very important for pest infestation mitigation through application of physical control, cultural control, chemical control, biological control, crop plant resistance, among others (see UNDP & UNDRO, 1992: 44).

3.2.5. Impact assessment techniques

There are various techniques through which we can assess the impact of pest infestation on communities or people. These may include:

i.   Infestation incidence and severity assessment; and

ii.   Aerial and ground surveys of crops damage.

3.2.6. Individual safety measures

i.   Application of pesticide for the control of pest must be done with caution to avoid the atmosphere with poisonous substances. It is important to check if the (pesticide) products are registered and have not expired;

ii.   Ensure that your surrounding is always kept clean and tidy so that pests will not find it as a good habitat;

iii.   Avoid activities that promote environmental pollution with the aim of reducing depletion of ozone layer and highly warm temperature that can engender rapid development of some pests;

iv.   Cover your food properly and ensure that you always wash your plates, spoons and other kitchen utensils with detergent and water before use;

v.   Block all holes or passageway that rodents and any other pests can use to navigate into your household, and carefully apply pesticide whenever their presence is noticed; and

vi.   Educate members of your family on the need to control pests.

SELF ASSESSMENT EXERCISE

How will you analyse pest infestation as a security threat?

4.0   CONCLUSION

In the last two units, our focus had been environmental forms of security threat. In this unit, we have subjected environmental pollution and pest infestation as security threats into analytical scrutiny. Environmental pollution are of different types, which include air pollution, water pollution and soil contamination. Air pollution is often generated from emission of greenhouse gases into the atmosphere and one of its consequences is invocation of significant variability in climate conditions (climate change). Climate change also produces some contradictions that can engender the problem of environmental scarcity. Air pollution can also potentially undermine the health safety and security of people by inflicting them with variety of health problems including neurobehavioural disorders, cardiovascular ailment among others.

Water pollution can also attract waterborne diseases like cholera and typhoid. Soil contamination is also associated with environmental pollution, capable of making plants drastically lose yields while existence of mercury in this soil can increase the risk of kidney damage among the people that consume the food harvested from the contaminated land. Considering the destructive effects that environmental pollution may have on people, it is always pertinent to develop strategies through which it can mitigated or reduce the loss that may accompany its occurrence in a community. Like environmental pollution, pest infestation can also pose great danger to people. Apart from irritation that is associated with pest infestation, it can also lead to a rise in the spread of bacterial, viral and parasitic infections among the people, capable of creating a public health crisis. It is germane to develop mitigation approaches to arrest the problem of pest infestation if meaningful development and security are to be achieved in any community.

5.0   SUMMARY

In this unit, we covered another set of environmental security threat (environmental pollution and pest infestation), which we were not able to study in the last unit due to limited time and space. We began our analysis of the environmental threats under focus by defining the term, environmental pollution, and thereafter we analysed various issues that bother on the risk its occurrence portends to people or the community. The second subject of discourse was pest infestation. We defined it and analysed it as an environmental security threat.

6.0   TUTOR-MARKED ASSIGNMENT

    i.   Define environmental pollution and pest infestation; and

   ii.   Explain three effects of each of the two environmental forms of security threat.

7.0   REFERENCES AND FURTHER READING

Funk & Wagnalls Standard Dictionary. (1962) International Edition.

Kemp, D. D. (1998). *The Environment Dictionary*. London: Routledge.

Santos, M. A. (1990). *Managing Planet Earth: Perspectives on Population, Ecology, and the Law.* Westport, CT: Bergin & Garvey.

UNDP & UNDRO (1992). *An Overview of Disaster Management* (2nd Edition). Disaster Management Training Programme.

://en.wikipedia.org/wiki/Environmental_pollution. Retrieved on 20 October, 2009.

://library.eb.co.uk/eb/article-9109632. Retrieved on 3 April, 2008.

://nidm.gov.in/Pest_Infestation.asp. Retrieved on 9 October, 2009.

Error! Hyperlink reference not valid.. Retrieved on 20 October, 2009.

://www.tropical-rainforest-animals.com/Environmental-Pollution.html.Retrieved on 4 November, 2009.

MODULE 3   TYPES OF SECURITY AND APPROACHES TO THREAT MITIGATION

Unit 1:   Basic Types of Security I
Unit 2:   Basic Types of Security II
Unit 3:   Basic Types of Security III
Unit 4:   Civil Security Approaches to Threat Mitigation I
Unit 5:   Civil Security Approaches to Threat Mitigation II

UNIT 1

BASIC TYPES OF SECURITY I

CONTENTS

1.0.   INTRODUCTION

Security is a subject that has attracted a rapidly growing interest and concern among social scientists whereby a wide spectrum of issues on the subject have been studied. The subject (security) has nevertheless attracted new studies, which have produced new breakthroughs and findings in security approaches and methodologies. The importance of security cannot be overemphasised, considering the 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 a given community.

Meanwhile, in the next three units including this one, we shall be discussing most of the basic types of security that exist. Though, there are many types of security, which we may not be able to cover but most of them shall be explained in this course. The first type of security that we shall discuss is computer security. Owing to the growing relevance being enjoyed by computer in recent times, putting in place some measures to protect our computers from malicious intrusion, malware and other forms of damage is very necessary and not debatable. It is against this background that we shall beam our searchlight on the subject (computer security).

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 computer security. A 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 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](://en.wikipedia.org/wiki/Computer_security)).

Computer 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 with it (**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 or 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 with 'confidential' label and the irony of all, 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. Such a situation may have a security implication on the State. For instance, a pensioner who has a number of children in tertiary institutions, and he is unable to have his entitlements because his file cannot be traced. Thus, that poor retiree will not have any money, if he does not have any other means of survival, to take care of his family. In this case, 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 the system that denies their father of his entitlements, the problem that 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 will not develop negative emotions, which can sometimes lure them into

social vices. I can remember a colleague of mine in 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 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 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 storage and maladministration of information. There is no doubt that absence of proper management of information can provoke a security threat in any State.

However, through the use of computer, the long queue and frustration that attend 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 space 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 and computers have gradually replaced them. It is no surprise that the management of many organizations in Nigeria have begun to mandate their staff to undergo various computer trainings in order to remain relevant in their various work places. Many public workers can now use computers effectively, as many government jobs 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 platforms.

Also, the Immigration Services in Nigeria has gone computerized. The processing and issuance of passport is now done electronically. The process appears to be faster and more convenient. Now, let us consider a scenario where the details of all those who have applied for Nigerian passports in the last two years got 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, it is important to provide adequate security for our computer system(s).

Therefore, essential measures and applications must be put in place, to secure our computer system especially as security experts. The nature of 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 discuss various ways to secure our computers but before we do that, let us quickly explain key concepts of computer security in order to stimulate our better appreciation of the subject.

SELF ASSESSMENT EXERCISE

Describe the term computer security.

3.1.1 Key Concepts in Computer Security

Anti-Virus Software: There has been a conflict among scholars on the originator of anti-virus software but the history has shown that the first public virus removal task was performed by Bernt Fix in 1987 (see 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 the sites that are not secure, or those designed to perpetrate scam online, through prompt alert and warning of the imminent danger such sites pose to the user and/or system, and it will advise that the user should not give the details of his/her vital information or better still 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, and the list may include Norton, AVG, McAfee among others. Due to the way new virus are generated almost on a daily basis by malicious people for commercial, strategic or any 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 malicious 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 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 computer virus through the use of recordable or rewritable discs but now the story is different. Computers get attacked by viruses, Trojan horse and worms if they are not well protected. 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 been used somewhere else especially 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 your anti-virus package on your computer system.

Authentication: This involves a technique in which we create password to restrict access of people to one's computer. In this case, it is only those with correct password who 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 authorisation, 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 (://www.webopedia.com/TERM /a/authentication.html).

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 computer 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 which allows in secure system, vital algorithms as well as code to be proven mathematically through which the specification of the computer can be met.

Backups: These are simply 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 as the same as mine.

Capability and Access Control List: These techniques are often 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 being transmitted from one system to another or from one place 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 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 the 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 unreadability of the information that can read through the content of the message. This approach can be used to send secret or very confidential information to several people irrespective of their number in as much as they have cryptographic key, which will enable them to decrypt it.

Decryption: Decryption can be defined as the tool used with the aim "…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 privilege 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 to use 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 privilege that "where an entity has only the privileges 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 whereby each of the units is designed less complicated, which 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 to detect and determine the nature of breach, its degree and the time it occurs. Audit trials should be stored very discretely 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 artefacts 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

Introduction of computer to the world population has really affected the culture of information generation, storage and amendment among the 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 convenience, 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 that 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 stressed 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   TUTOR-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 2

BASIC TYPES OF SECURITY II

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Body
        3.1   Meaning of Information Security
                3.1.1   Approaches to Information Security
        3.2   Meaning of Physical Security
                3.2.1   Approaches to Physical Security
4.0   Conclusion
5.0   Summary
6.0   Tutor-Marked Assignment
7.0   References / Further Reading

1.0   INTRODUCTION

In this unit, we shall continue our search for 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 introduce a new set of forms of security to the reader. The two forms of security that we shall consider in this unit for our study include information security and physical security. In that case, let us quickly highlight the various tasks we shall undertake 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 on 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 the mere electronic medium.

On the other hand, in computer security, the central focus is 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 they complement the functions and operations of each 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. Due to the opportunities provided by information technology revolution and recapitalization agenda of the Nigerian government, the financial sector is proactive in increasing their capital base and improving on their information system. The emergent information technology breakthroughs 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 the traditional way of counting money by the cashiers (now we have money counting machines).

Nostalgically, I 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. Sometimes, one gets to the bank early and finds 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. Now, with the introduction of ATM, people can withdraw money electronically anytime and anywhere, and the interswitch nature of the ATM has further made it easy for people to cash their money.

The era of traditional restriction to one's bank appears to be no more. A Wema Bank customer with interswitch ATM can cash his/her money in an ATM platform mounted at any First Bank branch or other banks. Even, the modern information technology allows one to transact business, trade and do some shopping online in a corner of your home.

However, considering the opportunities provided by the modern information technology, financial transactions, trading, information exchange, mailing, communication etc, have been made so easy. You should note that there are always two sides to a coin. Though, there is so much convenience and fun derivable from modern information system, it can be awful considering the amount of risk and danger in it. 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, loss of money can occur.

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 collapse for suffering malicious attacks like 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) <u>Confidentiality</u>: 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 so seriously. They need to know that it is very essential to prevent the very vital information of the organization 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 wrong hands or unauthorized person(s) or system(s), it will amount to a breach of confidentiality.

Let us use an ATM transaction as an example. You may decide to procure a standard international passports, for the reasons best known to you, and you are aware that you can do your application online, then you log-on the website of the Nigerian Immigration Services 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 the 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 or during or after the time of making the 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 whom you transact business, 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 your ATM details especially the pin-code during the transmission, and which are stored in a very secure location with very 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 right to institute a legal action against such erring organization for a breach of confidentiality.

Again, if your spouse is allowed to access the statement of your bank account without being authorized, it is also tantamount to 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. For one having the right to sue for a breach of confidentiality involving his/her own spouse, what justification does a stranger or a distanced person have in having access to one's information without authorization? This simply shows 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 the importance of information, the approach of **due care and due diligence** has been adopted 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) <u>Integrity</u>: Integrity can be described as a way of protecting information by restricting access permission 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 exposure of the system to malicious attacks.

Undoubtedly, this kind of violation occurs in many organizations where employees exhibit non-challant 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, even neighbours visit some employees, and many of these visitors may be allowed to use organisation's computers especially when they are connected to the internet. These persons use all sorts of storage facilities to down load 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 access to information, which ordinarily they are not supposed to access in the first instance;

C) <u>Availability</u>: 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, 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 they demand that necessary mechanisms be brought to bear to prevent disruptions that may result from hardware failures, power outages, physical destruction of the information systems, to mention a few;

D) <u>Authenticity</u>: 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 through this way we can have reliable and quality information;

E) <u>Risk Management</u>: Everything about life is a risk. There is risk in the relationship between two or more people, even within oneself. 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 everyday business of every man. Sometimes, we decide in the middle of the road to see a loved one in his/her place of work, even after notifying him/her of our intention, yet a conscious mind will still have a doubt in meeting him/her at the office because every second is clouded with eventuality. It is possible that the receptionist will just 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 you on phone.

Considering that scenario, risk is the second nature of 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 to its information system.

Furthermore, in as much as 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" ([://en.wikipedia.org/wiki/ Information_security](://en.wikipedia.org/wiki/Information_security)); and

F) <u>Information Classification</u>: There are different types of information in information system, and there is a need to classify according to their level of importance and confidentiality. By doing this, we will be able identify the amount of protection to be accorded to each of these available information. For the purpose of engendering the culture of information security, it is imperative for organisations 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 should not see himself as a 'man of God' and a good husband while he has some extra-marital affair with a former female staff whom he communicates with from time to time. May be because he is not exposed to good use of internet and he always asks his male secretary to help him with the mails to his 'lady-friend', and mandates the secretary to classify the mails as **top secret**, giving more importance to it than the very important information of the organization. This example reflects a clear case of misuse of office and misclassification because it is abnormal to place private issues above those that concern the organisation in a work environment.

Within an organizational setting, we classify information based on the value each of it has to the organization. In private organizations, classification model usually labels 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 the 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 facilities. For instance, there are some computers that will demand for your biometric information before you are granted access into it. When we

talk about biometrics, it is not actually about username or password, the security technology of biometric usually involves hi-tech security measures especially where 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 of forcefully gaining 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 from the ATMs is usually an effort in futility because, even, if 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 for 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 from 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 will you describe physical security?

3.2.1 **Approaches to Physical Security**

In summary, 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 obstacles or barriers that can prevent the potential attackers or intruders or malicious personalities from gaining easy access into the facility. The attackers, be it accidents, environmental disaster or human attackers will be impeded by putting in place some measures like multiple locks, fencing, walls, fireproof safes, and water sprinklers, to mention a few;

(b) The second perspective to physical security is 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 such fire incidents, it is expected for us to have fire-fighting equipment or call professional fire-fighters to come to rescue in quenching 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 to 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, 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 or divisions or areas in security sector. In this case, it is expected to do the placements to various available departments according to 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 that attracted our attention was information security. Consequently, we explained the meaning of information security, and as its various approaches were also explained. Thereafter, we beamed our search-light on 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   TUTOR-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).   *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 3

BASIC TYPES OF SECURITY III

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Body
       3.1   Infrastructure Security
       3.2   Seaport Security
       3.3   Airport Security
           3.3.1   Elements of Airport Security
       3.4   Food security
       3.5   Health Security
       3.6   Economic Security
       3.7   Environment Security

4.0   Conclusion
5.0   Summary
6.0   Tutor-Marked Assignment
7.0   References / Further Reading

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 explain 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 this unit, let us quickly look at the objectives of the study. This, we shall do in the next segment of the unit.

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; and

- 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, Central Bank, dams, oil refineries among others. Highways and bridges are also an aspect of critical infrastructure (://www.tsa.gov/travelers/highway/index.htm). Due to very high importance that these infrastructures have 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 is poisoned, so 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 the tendency that it can easily be attacked by terrorists or saboteurs. Similarly, 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 the infrastructure. it is a matter of fact that any damage intentionally or accidentally done to the critical infrastructure will have far-reaching effect on the economy and overall security of the country. For instance, the continued destruction of gas pipes often disrupts level of power supply in the country with serious consequences for the power generation capacity of the Power Holden Company of Nigeria (PHCN). The threats that 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 fails 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 will be vulnerable to threats especially if enemies bring into the country materials that are harmful and destructive.

Take for instance, if there is no provision of sufficient security at the seaports, there may be a situation of proliferation of weapons and small arms in that country, and terrorists can easily operate where there is no adequate security at the ports. Here, enemies can easily hide destructive objects like bombs, guns, chemical weapons among others in the containers, which they may later use against the country. This view is shared by Greenberg *et al.*, when they state "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 **Error! Hyperlink reference not valid.**). There is no doubt that any poor security handling of cargo can expose the country to security risk.

For instance, in a country where there is sharp ethno-religious division like Nigeria, circulation of such weapons can engineer insurgency and growing criminality as experienced in the country in recent time. The level of sophistication in armed robbery operation and the weapons the bandits use in recent time, calls for total restructuring 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**

Airport is a place that involves an aspect of transportation. People travel either by road or sea or rail or air. All these means of transportation deserve to be provided with sufficient security. It is no exaggeration that airport has continued to receive greater attention due to very strategic reasons. One of the reasons is that it is the most popular means of transportation, it is the fastest. And apart from being a means of moving people from one destination to another, it is also used in 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 as those who escort travellers to departure lounge 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.

Another reason is that airport 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 the security in their airports with the aim of making their airports less vulnerable to any enemy's attack. Previously, less attention was paid on screening the passengers for the possession of small 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 those disgruntled elements who often call themselves freedom fighters

The list of terrorist attacks through airports is long. One of such terrible occasions was a Cubana Flight 455 flying from Barbados to Jamaica, which was attacked by terrorists on October 6, 1976 where seventy-three people were murdered. Another case was Air India Flight 182, which experienced bomb attack that led to the killing of 329 innocent people. On 30 May 1972, a gang of three terrorists who were linked to the Japanese Red Army, shot and threw grenades at people sporadically at Lod Airport (now Ben Gurion International Airport) in Tel Aviv, Israel. Before they were overpowered, they had already killed twenty-four people as no less than seventy-eight people sustained various degrees of injury.

Again, in December 1985, the Rome and Vienna airports also 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 leading to the killing of no less than 20 people. The most serious of all was the September 11, 2001 terrorist attack where some commercial planes were hijacked by terrorists linked to Al-Qaeda network that were deliberately crashed by the terrorists into the World Trade Centre and Pentagon while the one meant to be crashed on the White House 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 airports worldwide, various governments have began 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 the 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) <u>Airport security personnel</u>: The enforcement authority in the airports vary according to the class of each of the airports. There are first class airports that

can serve as international airport to be used as entry and exit point for travellers coming or leaving the country. Conventionally, an international airport must definitely satisfy 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 in 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 enough security personnel there. Unlike countries like the United States where state and local governments have 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. Well, the type of security personnel arrangement, you are likely to find at any international airport depends largely on the security policy of each country. For instance in Nigeria, there is absence of state police and no state government can provide security for any local airports without seeking assistance from the federal government. Generally, in airports, the security agencies that can be found may include:

❖ Policemen and officers specially attached to the airports;

❖ Situating a permanent police station at the airport stocked with adequate equipment and competent personnel;

❖ Members of the Public Intelligence Community like State Security Service (as in Nigeria) who will be stationed as 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;

❖ There must be the presence of some members of (other) paramilitary agencies like Immigration Service and Customs Service to identify illegal immigrants or immigrants considered a threat or importers/exporters of harmful and banned products, and the culprits should be arrested, investigated and if found wanting necessary steps should be taken to subject them to immediate prosecution;

❖ There must be the presence of emergency team at the airports that can respond timely and effectively to events of disaster like plane crash or fire outbreak at the airports;

❖ There must be the presence of anti-bomb experts at the airports to detect concealed bomb items or detonate any explosive found at or around the airports;

❖ Services of police dogs should also be secured for the detection of explosives, hard-drugs and dangerous objects;

❖ Location of military barracks near the airports 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 may not able to conduct the main screening at the screening points. They 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 (://wn.wikipwdia.org/wiki/Airport_security), and

(b) <u>Installation of security equipment:</u> 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 even knife and other sharp objects that can be used to harm the passengers and crew at 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 (EDT), and puffer machines. These machines are used to conduct screening of baggage and other travelling materials to detect if any has any explosive substance 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 pictogram sensitivity (see ://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 and weapons any passenger may have on him/her. 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 that used to be one of the greatest food baskets and a major exporter of agricultural products in the world has become a perpetual importer of food items, meaning that, adequately feeding the masses would be a difficult task. There is no doubt that the agricultural sector has become moribund. More than 70% of urban dwellers go about on empty stomachs. The pervasive hunger that rents the air has continued to make people 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, 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 the opportunity to provide the people with food in qualitative and quantitative terms. However, food security underscores the strategic importance that self sustenance in food production has on the security of any nation. Though, 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 will you explain food security?

3.5   Health Security

This involves safety against HIV-AIDS pandemics and other 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 the platform to promote healthy living among the people. Health security is very crucial to national development, and that is the reason 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 they 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 by educating the 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 the spread of disease(s) especially those with high contagion.

Also, in most states, sanitation officers are appointed by government to ensure strict compliance of 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, there are some governments that 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 job do not have any 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 youth.

SELF ASSESSMENT EXERCISE

How will you define economic security?

3.7   **Environment Security**

The concept of environment has begun to dominate international discourse. The issue of environmental pollutions has continued to attract attention among individuals, Non-Governmental organizations (NGOs), nations as well as international organizations. It is imperative, if we consider the adverse effects that environmental hazards may have on the people, for government and the people to 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 its (relevant) agency – the United Nations Environment Program (UNEP), to monitor environmental issues, and make reports and plants for such issues and make reports and plans for such issues and to act and promote legal instruments on the environment. If we want to talk about environmental security, our focus shall be on the atmosphere, lithosphere, hydrosphere and biosphere. People now talk about issues like damage in ozone layer, climate change, water pollution and environmental degradation (to mention a few). Environment has great impact on the general wellbeing 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 towards 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 different functions they perform by working collaboratively in 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 TUTOR-MARKED ASSIGNMENT

Describe 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

Greenberg, M. D., et al. (2006). *Maritime Terrorism: Risk and Liability*. Santa Monica: RAND Corporation. Cited on ://en.wikipedia.org/wiki /port_ security. Retrieved on 30 August, 2009.

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 4

CIVIL SECURITY APPROACHES TO THREAT MITIGATION I

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Body
         3.1   Definition of Civil Security
         3.2   Approaches to Civil Security: Introduction
         3.3   Risk Education
         3.31   Elements of Risk Education
4.0   Conclusion
5.0   Summary
6.0   Tutor-Marked Assignment

7.0   References / Further Reading

1.0   INTRODUCTION

The issue of security has been very germane to the peaceful cohabitation of the 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 discuss the meaning of civil security as well as other areas of discourse pertaining to it. Due to the 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 explain 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 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" (**Error! Hyperlink reference not valid.**), it is imperative to adopt civil security framework, which will enhance the capacity of the public to act on their own in the time of emergency and hazardous events.

How do you describe civil security? Civil security can be described as any conscious measures 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 those that are 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 is very evident in the contemporary world. This view is supported by President John F. Kennedy several decades ago, at the height of 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, 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 helpless in taking care of themselves in the event of security threat.

Shalamanov *et al*. (2005) present a different perspectives to the definition of civil security and according to them civil security can include 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 the 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 will 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. So, what are these approaches? They include the following:

   a) Risk education;
   b) Preparedness;
   c) (Public) Warning; and
   d) Protective Actions

Civil security involves a network of activities, it demands connecting various approaches that are brought into 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
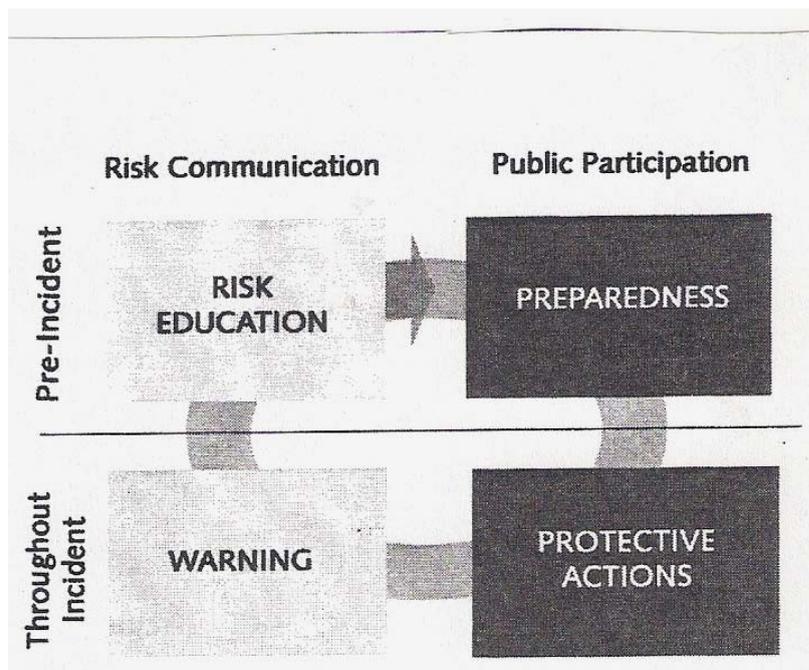
Source: Dory, A.J. (2003a). *Civil Security: Americans and the Challenges of Homeland Security*. Washington DC: CSIS.

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.

And having educated on 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 the public to issue warnings by alerting or notifying them of the occurrence of a hazard, and the steps they should take to forestall the disaster that may result in huge loss of lives and property.

Also, in a situation whereby a hazard or attack occurs, the security sector communicates 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 in a community, the government may reasonably decide to quarantine or restrict everybody coming from such a 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, 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 materials are the outcomes in providing utility. Thomas Hobbes contended people's resolve to take the risk of surrendering their sovereign power to a central Sovereign entity because of the brutish and nasty nature of the Hobessian state. Though, uncertain of whether their lots would be better or not under the new arrangement due to perpetual absence of security of lives and property that existed prior to convocation of sovereign political authority in 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 convocation of 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 at 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 it out to make money. His/her desire is to use the money got 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 candle on the table and in the twinkle of an eye, the house is engulfed in flame. 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 education of risk 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 the financial capacity to do such. Even, if taken to court, little can be done to prevail on the careless tenant except he/she has the means to provide the landlord-retiree 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? You answer is as 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 a 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 the 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 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. 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 effect 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 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, no doubt, shows the existence of risk in the relationship not only between a man and woman but among the 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 will you describe risk education as an approach to civil security?

3.31   **Elements of Risk Education**

a)   Development of unclassified national intelligence: There is need for government at the center 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, that 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 actions. 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 not at ease'.

It is important for intelligence agencies to educate the 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 were abandoned by their former patrons with no efforts by these callous politicians to retrieve the weapons from thugs.

Unfortunately, the youth, after being abandoned by their former masters became frustrated, and began to devise means for themselves to survive especially when they have understood the dynamics of the economics of violence. So, many of them became armed robbers, kidnappers, saboteurs, to mention a few. The elites and their relations have now become the main targets of kidnappers, a situation, which speaks volume of the risk inherent in the 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, 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) was alive to its responsibility not only to prevent such institutions but also to provide 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 any 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 is supposed to

provide guidance to government and the public on how the activities of these wonder banks posed a great risk to the security of the public failed in discharging its duties in this respect. It is laughable that many government officers were also found patronizing those financial institutions due to their thirst for making quick money;

c) <u>Interactiveness in risk education</u>: It is imperative to make risk education interactive, so that the process will be participatory. In this case, the government should provide various fora through which individuals and respective security agencies can meet to discuss and brain-storm as well as to enlighten one another on different threats and appreciate the risks such threats pose to security management of their communities. These fora may include town halls, 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 the Nigeria Police has adopted the strategy of bridging the gap 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 understand possible threats to security of the community at large. For instance, in many communities, people are ignorant of the risk of mounting high fence in their houses for security reason. For instance, if someone is being robbed, how can the passers-by know that he/she is in distress? Meanwhile, 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 the security rescue teams i.e. Police to gain easy access in situation(s) of distress;

d) <u>Massification of Risk education</u>: 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) <u>Active Participation of individuals in risk education</u>: 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 you desire to have knowledge of by participating on security talk show especially when relevant security experts are invited to the radio or television programme. 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. Here, it will be highly unethical for such a Police chief to disclose such information because of its capability to undermining 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 measures, taken by stakeholders with the aim of reducing and addressing vulnerability to their security. It helps to educate the 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 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, the 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. The law-enforcement agents have been continuously of being an instrument in the hands of some politicians to rig elections and repress the public that it is supposed to serve.

5.0   SUMMARY

In this unit, we began our academic journey by examining the meaning of civil security by looking at some of the existing definition of the concept. Though, the concept is new in security studies and practice but a 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 beamed our searchlight 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 unit, we shall discuss other three 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 only if it is very necessary. Good luck.

6.0   TUTOR-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 APPROACHES TO THREAT MITIGATION II

CONTENTS

1.0   Introduction
2.0   Objectives
3.0   Main Body
        3.1   Preparedness
        3.2   Public Warning
        3.3   Protective Actions
4.0   Conclusion

5.0   Summary
6.0   Tutor-Marked Assignment
7.0   References / Further Reading

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 in playing complementary roles not 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 discuss 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 in supporting 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 the 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 to occur, and in a 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 that preparedness is very fundamental to safety and security management. We cannot but agree with the Boy Scout in their motto, which is '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 of constituting a security threat to the whole people, the

people act swiftly by asking the fellow to vacate the place or he will be handed-over to the police.

In situation of an armed robbery attack, the people jointly put-up a strong resistance against the attackers whether or not the attackers aim at 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. 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 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, heart-quake among others.

It is very unfortunate that in Nigeria, neither the security sector nor the civil public is adequately trained to respond promptly and effectively to 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 nooke 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 in 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 the 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 the 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 the Nigeria Police are poorly equipped. This is instrumental to their poor state of preparedness activities. It is most disturbing the way police stations are being attacked in recent time. 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, 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 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 for safety.

SELF ASSESSMENT EXERCISE

How will 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, especially 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 the 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 take proper 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. You should know that disaster involves huge loss of lives and property, which should be avoided as much as possible. What determines 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 must be analysed. After the analysis, we can therefore take 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 people's 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. If it is found at the end of the day that a 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 but also by 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 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 will be necessary to translate the warnings into the local languages of the target population. Where some 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 they 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 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 to be 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 case entirely for the people to whom the warnings are issued, 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 the 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 other three 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 sometimes through carelessness or recklessness as the case may be or human error. For instance, some people are found in the habits 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 in Ikorodu, Lagos state still lingers in the memory of many Nigerians especially the families, friends and close relations of the victims where the fire-outbreak 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 volume 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 erring employers including life imprisonment.

Again, the issue of terrorism should be given priority attention by Nigerian government. If incidence of terrorism is less evident or not existing at all in the country now it 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. Here, 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, so 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). 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 a crucial element 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 of the 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 persons 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 have been 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 the issue concerning their safety and security. For instance, in Nigeria, many people have died when the boats they were travelling in 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 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

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 to 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 learn ways to take care of themselves 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 hazard more creatively and effectively too than any 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 no 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   TUTOR-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   MEASURES FOR THREAT MANAGEMENT

Unit 1:   Risk: Meaning, Psychology & Analysis
Unit 2:   Vulnerability and Capacity Assessment
Unit 3:   Simulation in Law Enforcement
Unit 4:   Crime Analysis: Meaning and Importance to Crime Mitigation
Unit 5:   Applying Data Mining and Automated Data Analysis for Crime Management

UNIT 1

RISK: MEANING, PSYCHOLOGY & ANALYSIS

CONTENTS

1.0   INTRODUCTION

Risk features in every aspect of human relations as well as various fields of human occupation. When we talk about risk, we need to know that it is a concept that is not limited to any specific actions or professions. It is against this background that the Red Cross (2000: 6-7) contends that:

Risk is defined differently by people in different situations. Risk, as perceived by the politician or the disaster manager, is different from risk as understood by a scientist, or by an insurance company salesman, or by a family living in an earthquake zone (Red Cross, 2000: 6-7).

Despite conceptual differences and in as much as we cannot do away completely with, it is pertinent to put in place measures and approaches through which we cannot only analyse the risk but also assess it in identifying how much capacity we have as a people or professionals to mitigate the effect of any hazardous events. Thus, the lower our vulnerability to any particular hazards or threats the lesser the risk we may encounter in case we experience such hazards or threats. In security profession, we face quite a number of risks in the discharge of our duties.

For instance, one may be leading an anti-riot security team mandated to arrest any breakdown of law and order that can result from a protest. At a point, one may find himself/herself in a dilemma in his/her choice of instructions to be given to his/her team in arresting the riot situation. It is incumbent on the security team leaders to exercise caution in issuing instructions because of the risk that may pervade every action of his /her team in quelling the riot. This will therefore necessitate putting available options to risk analysis before finally arriving at the actions that might be considered most appropriate to arrest the situation. Sometimes, simply cajoling the rioters may be the better option rather than application of force. In this unit, we shall focus on the meaning of the concept of risk and other important issues of discourse including risk psychology, risk analysis and risk evaluation.

2.0   OBJECTIVES

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

- Define the term risk;

- Explain risk psychology; and

- Discuss risk analysis.

3.0   MAIN BODY

3.1   Meaning of Risk

Risk can be simply described as any possible effect of a loss resulting from a hazardous event or an attack, which "can be expressed as a product of the consequences of an event and the probability of its occurrence" (Dory, 2003: 23). Politically, there is national security risk in countries where ethnic flag or religious association is used as a platform to secure employment and any other state resources. As you may be aware, African countries including Rwanda, Burundi, Nigeria, Kenya among others where the incidence of ethnicity has been very evident, have continued to be on the brink of state collapse due to intermittent ethnic violence as nation-building appears to be a scarce commodity.

The overall problems that may emerge from such ugly situations may include risks that involve breakdown of law and order, civil strife, coups and countercoups, continued underdevelopment, poverty and starvation, unemployment, and maladministration, to mention a few. There is no doubt that the incidence of risk becomes increasingly imminent as the consequences of an hazardous event are increasingly experienced with (very) little or no capacity to mitigate such threat or hazard or attack. A good example is the problem of growing rate of crime and criminality among youth resulting from job-drought (massive unemployment) in Nigeria. Undoubtedly, since the 1980s, Nigeria has been experiencing abominable rate of violent crimes and intermittent ethno-religious violence, and the reasons for these problems are not farfetched.

One major reason is economic quagmire occasioned by maladministration, paradox of the monolithic oil economy as well as corruption. Other factors may include the endemic culture of patron-client network in our political life, religious fundamentalism, ethnic and tribal intolerance, among others. Nevertheless, all these factors constitute a great security risk to the survival of the Nigerian-state as the country often experiences ethno-religious tension with high casualty rate and huge generation of internally displaced persons. Also, the crime situation in the country, is worrisome as blood-sucking phenomenon bank robbery, kidnapping and politically-motivated assassinations has been most visible in the last ten years in Nigeria. How do

you describe the term risk? Although, there are several definitions of risk but we shall consider some of these available definitions. Simply put, risk can be described as:

...the expected or anticipated losses (lives lost, people injured, property damaged, and economic activities or livelihoods disrupted) from the impact of a given hazard on a given element at risk over a specific period of time (Red Cross, 2000: 6).

...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.**).

...a measure of the expected losses due to a hazardous event of a particular magnitude occurring in a given area over a specific time period. Risk is a function of the probability of particular occurrences and the losses each would cause (**Error! Hyperlink reference not valid.**).

...the threat or probability that an action or event will adversely or beneficially affect an organization's ability to achieve its objectives (Luhmann, 1996 on **Error! Hyperlink reference not valid.**)

...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 (://www.unisdr.org/eng/public_aware/world_camp/2004/booklet-eng/Pagina 9ing.pdf).

...the expected lives lost, persons injured, property damaged, economic activity disrupted due to a particular hazard. Risk is the probability of a disaster occurring and resulting in a particular level of loss (UNDP & UNDRO, 1992: 74).

Considering all the foregoing definitions of the term risk, we can summarise risk as follows:

Risk = Consequences of events x Probability of Occurrence

Meanwhile in disaster management, risk involving the transition of hazard into a disaster can be summarised as follows:

Risk = Hazard x Vulnerability

Again, in engineering, risk is defined simply as:

Risk = Probability of an Accident x losses per accident

As we have rightly argued in the introductory segment of this unit, there is no way we can absolutely or totally do away with risk, even if we try to avoid risk, we are at the same time, taking a risk in our choice of actions or decision to do away with the risk. Therefore, we can only reduce or manage the incidence of risk in our relations, businesses as well as actions. For instance, one may decide to fortify the security of his/her house with very high fence to prevent burglars and any other attackers from jumping into his/her compound through the fence but most times, people forget to consider the risks that are involved in mounting high fences.

Apart from preventing passers-by to know if the occupants of such high fenced buildings are under any attack by enemies like robbers, these high fences also constitute a high security risk because of the potential danger they pose to the occupants and even passers-by in case these fences collapse. As you may have heard, quite a number of people have been killed or injured due to the collapse of high fences, which fell on them. The simple risk arithmetic here is that the more fortified a security fence, the more harm it can potentially cause, if it collapses on any person(s). This brings us to the subject of **risk probability**.

Risk probability is often regarded as a way of quantifying the intensity of a risk in generalised way. For instance, we can generalise that the probability of having youth posing huge risk to the national security will be high where there is massive unemployment. The fact is that due to adolescent anger, youth express more aggression than the elderly (see Fuller & Forrest, 1990; Goldstone, 2002; Urdal, 2004). Another example is that there is probability that 1 out of 200 smokers that take (on average) 10 cigarettes a day will die of smoking-related ailment(s) like lung cancer. We can also argue that in Nigeria, 10 out of 300 policemen on patrol without wearing bullet-proof vests face the risk of being killed by armed robbers or any other malicious attackers. There is no doubt that such gross risk estimates can be very helpful for comparative reasons but it mostly covers-up huge "variations in the risk to individuals or different regions" (UNDP & UNDRO, 1992: 74).

SELF ASSESSMENT EXERCISE

How will you describe risk?

3.2   **Risk Psychology**

With a view to find answer to why a number of persons usually derive satisfaction from always engaging themselves in actions and activities that involve high risks, psychologists have carried out a lot of research inquiries but virtually none of the existing studies has shown "...how a risk taking impulse arises from within or what role is played by environmental factors, from upbringing to the culture at large" (://www.psychologytoday.com/articles/199411/risk). It is always very surprising to still see quite a number of technicians or engineers in Nigeria's National Power Holden Company working on faulty transformers without the use of any protective equipment like hand-gloves despite the fact that many staff have died through

electrocution resulting from unnecessary risk taking by not wearing any protective materials like gloves to mitigate electric hazard.

Similarly, many people buy new cars without having any consideration for insuring their new vehicles against any incident of theft or accident despite the fact that they know that vehicles are reported stolen almost on a daily basis in Nigeria. If you advise such people to do the right things like having insurance policy for their vehicles, many of them may say that it is not in their portion to experience such hazard or threats like car theft or accident. The question is: whose portion is the experience of such hazards or threats? With the growing false religious consciousness among the people, people now take, with impunity, high risks without considering the consequences that such risky behaviour may have on them. It is very sad the way some of the policemen in the country risk their lives and career by engaging in sharp practices even when they are not on official duty.

A good example was a bloody robbery incident that took place somewhere in Oyo state in 2009 where it was alleged that the policemen that were escorting a bullion van carrying money for an organisation were contracted unofficially and the security team was ambushed by the armed robbers. At the end of the day, more than five policemen were killed as the robbers carted the money away. It was very pathetic that the families of those slain policemen would not be entitled to any financial benefits from the government because the policemen were not on duty but doing their private (brisk) business at the time, they were killed, so their families will be entitled to nothing. Considering the foregoing instance, you will appreciate the high risk involved in engaging in actions, as security practitioners, that expose us to danger. At this point, let us quickly look at the definition of risk psychology. According to Amanda Dory, risk psychology can be described as:

...the ways in which individuals process and respond to risk information based on beliefs and emotions (Dory, 2003: 21).

...far more than a simple "death wish". Studies now indicate that the inclination to take high risks may be hard-wired into the brain, intimately linked to arousal and pleasure mechanisms, and may offer such a thrill that it functions like an addiction (://www.psychologytoday.com/articles/199411/risk).
...the branch of psychology studying perceptions, attitudes, decisions and behaviours towards risk and how humans and animals take risks. (**Error! Hyperlink reference not valid.**).

Security attacks like kidnapping, terrorism, armed robbery among others are usually psychological in nature owing to the fact that attackers often use instruments of coercion and dangerous weapons to carry-out their operations. They tend to intimidate their victims and attempt to do same to security practitioners or operatives especially the police with a view to perpetrate their evils and acts of criminality without hindrance, and these violent attacks can cause emotional problems like fear, anger and sorrow among the victims and security practitioners.

The very violent nature of crime in recent time in Nigeria and elsewhere has become a source of worry not only among the security practitioners or personnel but also among the civilian population at large due to the palpable security risk that such criminal activities constitute to the wellbeing of the general public. For instance, bank robbery occurs more frequently in recent time than ever before with equalled level of fatality and bloodshed. The frequent attack on members of the Nigeria Police has forced many policemen to always be in mufti due to the risk associated with wearing of uniform in the public.

The psychological problem emanating from the perpetual risk that dominates police job today has created a culture of jingoism and aggression among policemen whereby they often pull the triggers whenever and wherever some individual(s) is perceived as a threat without trying to find out if the person(s) is actually a threat. In the process of doing this, many innocent civilians have been killed by trigger-happy policemen in a situation that has further damaged the image of the police among the general public. Psychologically, in taking any risks, we need to consider the following by weighing them against each other:

Elements of Risk Psychology

a) Gain vs. Loss: As security practitioners, we need to always consider weighing how much gain we hope to achieve against the loss we may encounter in the concerning action(s) we are about to take. As earlier narrated, the story of some policemen who were killed by the robbers when they were making some brisk business, had it been that these fellows weighed the benefits (gain) they would derive from their illegal duties against the entitlement they would lose as well as other potential losses like loss of lives, I strongly believe that some of them would have decided not to partake in such illegal duties;

b) Cost vs. Benefit: Again, before we undertake any risky situation, we should endeavour to measure the size of the cost of our actions against the benefits that we hope to derive from such actions. For instance, Nigerian government always fails to conduct cost and benefit analysis before embarking on humanitarian interventions in Africa and elsewhere. Most times, we usually consider our position as a leading nation on the continent and with a view to tell the world that we are sisterly to the plight of other African nations, we often spend huge amount of resources in human and material terms in peacekeeping on the continent (cost).

There is no doubt that Nigeria through its humanitarian activities is being regarded as regional power (benefits) but these benefits don't translate into economic fortunes for the country as it continues to grapple with growing unemployment, youth restiveness, incessant ethno-religious violence, violent crimes, rituals, human trafficking among others. These problems are largely

economically-motivated and rather than using the larger part of the money being wasted on humanitarian intervention to address its internal problems, the government of Nigeria usually squanders it on peacekeeping.

It is no exaggeration that in the last two decades, Nigeria has spent more than US$ 2b in human and material terms on peacekeeping in West Africa, and due to its inability to effectively handle its internal crisis and endemic underdevelopment, she is often seen as a laughing stock in the comity of nations. There is a general saying that Nigeria imports what she has and exports what she lacks, and it is most pathetic that most of the beneficiaries of Nigeria's philanthropy on the continent have appeared to be challenging its relevance in international diplomacy. For instance, apart from mounting some stringent conditions for the procurement of visa among Nigerians, South-African government also fails to safeguard the security of lives and property of Nigerian nationals staying in South-Africa despite the huge resources that Nigeria committed to its anti-apartheid struggle. The country is also one of the challengers of Nigeria for the permanent seat of the UN Security Council seat;

c) Threat vs. Opportunity: It is also important to ensure that adequate efforts are made to measure those external conditions that can hamper our objectives (threat) against those conditions, which can assist us in meeting our objectives (opportunities). It is by doing this that we will be able to know the amount of risk involved in our choice of actions. As security practitioners, some of us who are in the military may be mandated to undergo a peace enforcement exercise in a warring community.

Here, the opportunity we have may be our military preparedness and superior skills and equipment (opportunities) that make us to have a strategic advantage over the combatants (parties in dispute) but the truth of the matter is that having little knowledge about the topography and terrain of the warring zone (threat) may undermine our capacity to achieve our overall aim in the affected place and the loss of battle (risk);

d) Risk vs. Reward: Before we adopt any actions as regards our business, relationship and operations, we need to weigh the risk involved against the reward we expect from such actions. For instance, some criminal security-men or officers who are fond of renting out arms to armed robbers for monetary reasons (reward) actually fail to realise that these robbers may decide to use the same weapons to kill them (the erring security men and officers) or their close relations for any reasons which may include decision by the robber wishing not to return the weapons to the lenders (risk); and

e) Short-term vs. Long-term: It is also germane to weigh the short-term risk involved in our choice of actions against the potential long-term security risk

that such actions may portend before we conclude to taking any actions. For instance, successive administrations in Nigeria have paid a lip-service to the problems of environmental degradation and acute underdevelopment of the Niger-Delta region of Nigeria. The struggle which began in a peaceful or less violent way was largely mismanaged by the Nigerian governments especially the military regimes in the last thirty years in the name of natural security (short-term risk).

The government repression of the agitating groups of the region led to militancy, kidnapping and hostage-taking, which have had spill- over effect on the larger Nigerian society. The problem of kidnapping that was peculiar to the Niger-Delta has become a great security risk to the whole country as virtually all other regions are now grappling with the phenomenon of kidnapping and economic terrorism, which the nation's security sector has not been able to address as more criminal persons are going into the perceived lucrative business of kidnapping (long-term risk).

SELF ASSESSMENT EXERCISE

Explain risk psychology and its elements.

3.3   **Risk analysis**

Risk analysis is very fundamental to effective security management. In the conduct of security business, security practitioners encounter a lot of risks not only from enemies' attacks but also in our operations. And in as much as we cannot do away entirely with risk, it is pertinent to perform risk analysis. Summarily, risk analysis can be divided into two: quantitative or qualitative.

In **quantitative risk analysis**, we make effort to numerically determine the probabilities of a range of hazardous events and the likely extent of the losses if a particular event occurs. On the other hand, **qualitative risk analysis** does not actually involve determining any numerical probabilities but it is a function of identifying "the various threats, determining the extent of vulnerabilities and devising countermeasures should an attack occur" (://searchmidmarketsecurity.techtarget.com/sDefinition /0,,sid198_gci1182538,00.html). Operationally, there are various conceptual definitions of the term risk analysis. The list of these definitions is long, and we cannot be wrong to concur that risk analysis can be defined as a method that:
...involves analyzing target software for vulnerabilities and characterizing their nature and potential impact. Microsoft calls this "threat modelling." Risk analysis attempts to identify, prioritize, and plan appropriate mitigation for the risks facing a piece of software (://buildsecurityin.us-cert.gov/daisy/bsi/590-BSI.html).

Risk analysis can also be described as

...the process of defining and analyzing the dangers to individuals, businesses and government agencies posed by potential natural and human-caused adverse events ([://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci1182538,00.htm l](://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci1182538,00.html)).

A risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats (Wold & Shriver, 1997 on ://www.drj.com/new2dr/w3_030.htm).

...the systematic method of identifying the nature and causes of risks to which an organisation could be exposed and assessing the likely impact and probability of those risks occurring ([.etpconsulting.co.uk/Business%20Continuity/business-continui ty-glossary.ht m](://.etpconsulting.co.uk/Business%20Continuity/business-continuity-glossary.htm))

......the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards ([.ee.oulu.fi/research/ouspg/sage/glossary](://.ee.oulu.fi/research/ouspg/sage/glossary))

Elements of Risk Analysis

a. Investigating the regularity of particular types of threats: It is part of risk analytical tasks to conduct inquiry into the potential threats to security that are often experienced against the one that occur less frequently within a specific time and space. In Nigeria, it is often believed that towards festive periods especially Christmas the incidence of robbery usually increases posing greater risk to security of lives and property;

b. Classification of threats: There is also a need to classify the nature of threat in our risk analysis. The potential threats or hazards can be categorised as natural (flooding, seismic activity like earthquake, volcanic eruption, hurricane, tornado, to mention a few), technical (computing system failure, telecommunication failure, power failure, air conditioning failure, to mention a few), and human threats (assassination, bomb threats, computer crime, traffic homicide, chemical spill, industrial strike action, corruption, civil unrest, kidnapping, to mention a few).

c. Determining the level of predictability of the security threat: In identifying the risk involved in the occurrence of a threat, we should determine this by seeking to know how accurately we can predict its occurrence. Thus, the more accurate prediction we can make as regards its experience, the more we may be able to prepare towards mitigating it or reducing its impact on us, and consequently reduce the risk such threat may portend to us or society;

d. <u>Analysing the Speed of the onset of the threat or hazard</u>: In analysing the risk that characterises one particular threat/hazard or the other, we need to determine the swiftness or speed of the threat when occurring. There are some threats that happen very sudden, and these may include earthquake, floods, tsunami, and volcanic eruptions, to mention a few. Some threats may also be considered gradual in their occurrence, and these include drought, famine, environmental degradation, pest infestation, to mention a few. Thus, the speed at which the threat occurs determines its level if risk, as those threats that occur suddenly pose more security risk than those with slow or gradual onset;

e. <u>Determining the degree of warning or notification</u>: As part of risk analysis process, we should determine the amount of early warning and notification given by the threat or hazard before it occurs. For instance, it is generally believed that where there is lack of opportunity among the people to peacefully seek redress, violent settlement of disputes will become imminent;

f. <u>Estimating the length of time in the occurrence of threat or hazard</u>: In analysing the inherent risk of any threat, it is pertinent to do an estimate of the average time or the interval the threat or hazard usually occurs. By doing this, we will be able to determine the amount of risk that each threat poses to the security of a people or community;

g. <u>Impact Analysis</u>: In analysing risk, we are also expected to assess the impact of any given threat to general security atmosphere of any given community. We should be able to identify the amount of adverse effect that the occurrence of such threat or hazard may have on the general wellbeing of the people or /and infrastructure and/or community in general. Consequently, we will be able to measure if the impact of the threat will pose no or low or high risk to the security of the people or community. Thus, the greater the impact that a threat will have on the infrastructure or system or people the greater the risk it will pose to the security of the people or community or infrastructure;

h. <u>Discovering the consequences of a threat</u>: In conducting risk analysis, we are obliged to discover the potential consequences that the threat will have on people or community and these consequences may include infrastructural damage or/and loss of property or/and slight injuries or/and permanent injuries or/and deaths. The gravity of the possible consequences that the threat will produce largely deduce the amount of risk that such threat pose to security;

    i. <u>Determining the level of vulnerability to threat</u>: We should identify the level of our vulnerability to a hazardous event or threat to determine the amount of risk that such hazardous event or threat or attack can likely pose to security; and

    j. <u>Identifying potential risk mitigation factors</u>: This is a critical element of risk analysis. It involves identifying various ideas, approaches and methodologies that help in reducing the impact of security threat or possible ways to prevent its (re)occurrence.

SELF ASSESSMENT EXERCISE

Explain risk analysis and its elements.

4.0   CONCLUSION

Risk can be said to be part of human nature. We embark on one action (project or business or operation) or the other not without risk i.e. probability of it succeeding or failing. Newly married men often strive to get their wives impregnated with the aim of having the fruits of wedding, which are children but not without the risk that characterises child birth. Even, when the children are born safely, the parents face another risk of having means to provide for the basic needs of these children especially among families with little or no socio-economic fortunes. Professionally, as security practitioners, we encounter risks from time to time due to the nature of our job, and these risks can exhibit themselves from different dimensions like attacks from enemies (robbers, terrorists, arsonists etc), accidental discharge, blackmail, to mention a few.

For instance, there was a case of a security man who was mandated by his employer to shoot at someone who was thought to be a robber jumping into the compound through the fence, and the fellow never bothered to subject the instruction to risk analysis due to the mentality of most security men to obey superior orders without trying to know the rationale behind such orders (risk psychology). Incidentally, that security man shot the person mistaken for a robber and it was later found that it was the employer's son. Swiftly, the employer denied ordering the security man to shoot at the victim, and after a long judicial battle, the poor security man was sentenced to a long jail term after being convicted for manslaughter.

The fact is that many security men usually discountenance the possibility of being made liable to the actions taken by them despite being ordered to do so by their superior officers. The act of carelessly obeying the superior order without considering the risk involved in such orders is frowned at by international criminal law, recommending punishments for individuals who carry-out any inhuman acts for their "obedience to superior orders" (Bassiouni, 1992:343). It is therefore advisable to always subject all potential risks that we may encounter in our actions, relations and

professions to analysis, and it is when we do this (risk analysis) that we are likely to identify ways to mitigate the risks.

5.0   SUMMARY

In this unit, our central subject of discourse was risk and other related issues like risk psychology and risk analysis. We began our task by explaining the meaning of the term risk. Thereafter, we described the issue of risk psychology especially as it relates to security. The last area of inquiry was risk analysis where we defined the concept (risk analysis) and discussed its basic elements.

6.0   TUTOR-MARKED ASSIGNMENT

i.   Define the terms risk, risk probability, risk psychology and risk analysis; and

ii. Briefly discuss any three elements of risk analysis.

7.0   REFERENCES AND FURTHER READING

Bassiouni, M.C. (1992). *Crime Against Humanity in International Criminal Law.* Norwell, MA: Kluwer Academic Publishers.

Fuller, G. A. & Forrest R. P. (1990). Youth Cohorts and Political Unrest in South-Korea. *Political Geography Quarterly* 9: 9-22.

Goldstone, J. A. (2002). Population and Security: How Demographic Change can Lead to Violent Conflict. *Journal of International Affairs* 56(1): 3-22.

International Federation of Red Cross and Red Crescent Societies (2000). *Risk Reduction*. Disaster Preparedness Training Programme. Geneva: IFRC. June.

Luhmann, N.(1996). *Modern Society Shocked by its Risks*. Occasional Paper 17. Hongkong: Social Sciences Research Centre/Dept. of Sociology, University of Hong Kong. Available on ://hub.hku.hk/handle/123456789/38822. Retrieved on 30 September, 2009.

UNDP & UNDRO (1992). *An Overview of Disaster Management* (2nd Edition). Disaster Management Training Programme.

Urdal, H. (2004). *The Devil in the Demographics: the Effect of Youth Bulges on Domestic Armed Conflict, 1950-2000*. CPR Working Paper 14. Washington, DC: World Bank.

Wold, G.H. & Shriver, R.F. (1997). Risk Analysis Techniques. *Disaster Recovery Journal*. Available on ://www.drj.com/new2dr/w3_030.htm. Retrieved on 28 August, 2009.

://buildsecurityin.us-cert.gov/daisy/bsi/590-BSI.html. Retrieved on 4 October, 2009.

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

://kashmirdivision.nic.in/Disaster_Management_/dm_center.htm). Retrieved on 30 September, 2009.

://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci1182538,00.html . Retrieved on 4 October, 2009.

://www.oxfordrisk.com/about_us/risk_psychology.php. Retrieved on 1 October. 2009.

(://www.psychologytoday.com/articles/199411/risk. Retrieved on 1 October, 2009.

://www.unisdr.org/eng/public_aware/world_camp/2004/booklet-eng/Pagina 9ing.pdf. Retrieved on 30 September, 2009.

.ee.oulu.fi/research/ouspg/sage/glossary. Retrieved on 4 October, 2009.

.etpconsulting.co.uk/Business%20Continuity/business-continui   ty-glossary.htm. Retrieved on 4 October, 2009.

UNIT 2

VULNERABILITY AND CAPACITY ASSESSMENT

CONTENTS

1.0   INTRODUCTION

The function of responding to disasters is a very tasking one. Such a task involves adequate training and knowledge of various activities and action about disaster management. Due to the risk posed to the continued survival of every community in human and material terms, the subject of disaster management and emergency response is gaining more space within intellectual community. Quite a number of community-based efforts and initiatives are being undertaken by several local and international humanitarian organization especially the Red Cross and United Nations Disaster Relief Organization (UNDRO). The reasons are not farfetched, considering the degree of destruction in human and material terms that accompany any situation of disaster.

Take for instance, incident of inferno in private buildings, which is usually considered as minor disaster, is capable of destroying all that took an individual almost five decades to attain, just in few hours. In an occurrence of serious fire-outbreak, the occupants of the building may not have time to remove their valuable items and important documents like school results/certificates among other items, and within twinkle of an eye, all labour for several years can be consumed by fire. Considering the losses that may be recorded at domestic level through an outbreak of disaster, one cannot imagine the magnitude of losses that may be encountered in a major disaster like earthquake or tsunami, which effect goes beyond a single house but may affect the whole community or even several communities. It is against this background that

it is pertinent to always conduct vulnerability and capacity assessment with the aim of identifying threats that can constitute a disaster, so that we can further build our capacity to prevent or mitigate (the effect of) such disaster(s) as well as reduce the people's vulnerability to hazards. In this unit, our study interest shall be centred on the concept of vulnerable and capacity assessment (VCA).

2.0   OBJECTIVES

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

- Describe the term vulnerability and capacity assessment (VCA);

- Explain how VCA builds people's capacity to disaster mitigation and management through its objectives; and

- Discuss the importance of vulnerability and capacity assessment.

3.0   MAIN BODY

3.1   Definition of Vulnerability and Capacity Assessment

It is the aim of simplifying the concept of vulnerable and capacity assessment that we begin to delve into the conceptual task before us by separating the terms vulnerability and capacity, so that we can have better understanding of the subject under scrutiny. However, most times people and even humanitarian intervention practitioners mistake the concept- vulnerability for vulnerable groups. The regular misapplication of this concept (vulnerability) underscores the need to always subject the term to conceptual elaboration. The reason is that the term is wider in its meaning than to be defined parochially or narrowly.

Therefore, when defining the term, it is important to clarify within what context we are applying it. Though, in terms of economic distribution, poor people may be said to be vulnerable. Thus, this is not usually the case in disaster (management) discourse. This is because most times it is everybody, irrespective of one's socio-economic status, that will be affected directly or indirectly when disaster is experienced (Raphael, 1986), but the poor appear to be affected more than their rich counterparts. For instance, in a disaster where people's houses are washed away by flood, it will be easier for the rich to get another shelter than the poor because the rich have the money to get themselves alternative accommodation. This view is corroborated by Chambers (1989), who contends that it would amount to misconception if we mistake defencelessness or insecurity for lack of want, and according to him:

The contrast is clearer when different dimensions of deprivation are distinguished, for example, physical weakness, isolation, poverty, and powerlessness as well as vulnerability. Of these, physical weakness, isolation and poverty are quite well recognised, and many programmes seek to alleviate them; powerlessness is crucial

but it is rare for direct action against it to be politically acceptable; and vulnerability has remained curiously neglected in analysis and policy, perhaps because of its confusion with poverty. Yet vulnerability, and its opposite, security, stand out as recurrent concerns of poor people which professional definitions of poverty overlook (Chambers, 1989: 2).

The term, vulnerability can therefore be defined as:

...a perception of the lack of capacity to defend against injury, harm or damage from a threat or a hazard (Kuban & MacKenzie-Carey, 2001: 4).

...insecurity, the reverse of security"; it reflects *"the characteristics of a person or group in terms of their capacity to anticipate, cope with, resist, and recover from the impact of a natural hazard. It involves a combination of factors that determine the degree to which someone's life and livelihood is put at risk by a discrete and identifiable event in nature or in society* (Blaikie *et al*, 1994).

....the weakness in your safeguards to protect your assets (US National Institute of Standards and Technology cited by Kuban & MacKenzie-Carey, 2001: 4).

On the other hand, capacity can be said to be:

...based on specific requirements or needs and the distinct ability at that time to either employ or access needed resources. The assessment of capacity level is also a function of time and is typically modified over time, following changes to the operational environment or personal circumstances (Kuban & MacKenzie-Carey, 2001: 4).

From the foregoing definitions of the two terms-vulnerability and capacity, the former involves level of exposure of an individual or community to security threat or hazards while the latter deals with how much ability an individual or community have in mitigating the effect of a hazard and reducing the losses that accompany a threat or hazard, and more importantly the capacity to prevent the hazard from leading to a disaster.

At this juncture, let us see some of the existing definitions of vulnerability and capacity assessment (VCA). VCA as you are expected to know means vulnerable and capacity assessment. So, if you come across that acronym subsequently in this course or elsewhere, you should know what it means. And on the question of the definition of VCA, it can be described as a systematic and strategic way of measuring level of susceptibility to threats as against amount of ability available to counter such threats or hazard or at least to reduce losses, and the end result is to show if:

...individuals, households, communities and nations have resources that can resist the impact of a hazard and/or recover quickly from them. A hazard does not cause a disaster unless there are people affected by it; people who do not have the capacity to resist. For example, all countries of the world widely possess something very

dangerous: a system of roads with fast moving vehicles. But because we have some education and knowledge as well as faculties of sight and hearing we are not very vulnerable to this potentially serious threat. The fact that relatively few people get killed by walking across these roads shows the high level of training implicit in our up-bringing to avoid this hazard (see ://reliefweb.int/rw/lib.nsf/db900sid/LGEL-5G8F5Q/$file/ifrc-Toolbox-oct96.pdf?openelement
VCA can also be defined as a set of disaster management procedures:

...concerned with collecting, analysing and systematising information on a given community's vulnerability to hazards in a structured and meaningful way. This information is then used to diagnose the key risks and existing capacities of the community, ultimately leading to activities aimed at reducing people's vulnerability to potential disasters and increasing their capacity to survive them and resume their lives (IFRC, 2006: 4-5).

In addition, vulnerability and capacity assessment can be described as an approach, which reveals:

the extent to which a community, structure, service, and/or geographic area is likely to be damaged or disrupted by the impact of particular hazard, on account of their nature, construction and proximity to hazardous terrain or a disaster prone area (**Error! Hyperlink reference not valid.**).

In summary, the rationale behind VCA is to enable us to detect how much we are vulnerable to specific threats or hazards and what is the level of preparedness and how much resources we have to prevent the hazard from getting to disaster level.

SELF ASSESSMENT EXERCISE

How will you describe vulnerability and capacity assessment?

3.2   **VCA: Building Capacity of the Masses to Disaster Management**

In the last section, we revealed the misconception that most people have in the definition of the term vulnerability. This is because quite a number of people often use the concept exclusively to convene the pitiable situations that poor people are usually found. The meaning of the term transcends condition of poverty. In disaster management, it is not only the poor that may be affected by hazard or disaster as the case may be. This view is reflected in the words of President Carlos Flores of Honduras in his reaction to the very destructive effect of Hurricane Mitch that occurred in Central America in 1998, and according to him, "we lost in 72 hours what we have taken more than 50 years to build, bit by bit." (cited in 1FRC, 2006).

Meanwhile, one conclusion that can be drawn from the sorrowful comment expressed by Flores is that it is not the poor that are affected by the occurrence of disaster(s). The rich also cry, and the basis of this argument is that apart from loss of lives, most

of the houses and structures destroyed by the hurricane were owned by the rich. Therefore, in material matters, the rich suffer more than the poor when disaster is experienced but the recovery capacity of the rich is always greater than that of the poor.

The reason is that the poor are already vulnerable due to socio-economic incapacitation, and they become more vulnerable in the incidence of disaster. They hardly have enough resources to take care of their basic needs let alone having extra to use in the purchase of individual protective equipments to build their response capacity to hazard or threat. It is nothing but the truth that the level of vulnerability among the poor to security threat or disaster appears to be very high in developing countries like Nigeria. This situation is capable of undermining ability of the country to actualise the vision that behind the Millennium Development Goals (MDGs) (see ISDR, 2005).

Sadly, experience still shows that the country continually records avoidable deaths resulting from malaria and other common ailments. This shows that the poor are extremely incapacitated to mitigate losses from hazards and are also incapable of preventing hazard from getting to disaster. This gap between the 'haves' (rich) and 'haves-not' (downtrodden or poor) in their capacity to handle threats and managing disaster is one of the factors responsible for the introduction of vulnerability and capacity assessment by several emergency and humanitarian agencies notably the Red Cross.

Noteworthy, is the activities of such organizations have really attracted the attention of the international community, and the world body (the UN) through some of its specialised agencies especially the United Nations Disaster Relief Organisation (UNDRO). VCA is designed to reduce people's vulnerability and builds their capacity to disaster preparedness and mitigation through the following objectives:

a) Reduction of the impact of threats: one of the objectives of VCA is to assist people to reduce the impact or effect of security attack or hazards through mitigation, prediction and warning, and preparedness (see IFRC, 2006);

b) Capacity building: Efforts are made to enhance the capacity of the people towards reduction of vulnerability especially through risk education, preparedness, warning and protective actions;

c) Advocating for good governance: By advocating for good governance and abolition of all discriminatory policies and promotion of social justice and if the decision-makers begin to act creatively by giving the wellbeing of the people a priority attention, people will therefore have more self confidence and greater capacity to take care of themselves to reduce losses that may accompany any hazard or security attack.

For instance, if more employment opportunities are provided and living wages are introduced, people will definitely have more resources, some of which they can use to increase their ability to respond to hazards more creatively through risk education and by buying themselves some important individual protective equipment. For instance, a poorly paid worker whose car does not have a spare tire, upon having a substantial salary increase may decide to get a spared tire for his/her car. In doing so, he/she has improved his/her potentials towards risk reduction;

d) Addressing the structural causes of vulnerability: Poverty remains a factor that makes people to be more vulnerable resulting economic incapacitation. For instance, in most urban centres in Nigeria, many commercial motor cyclists still go about doing their business without the use of crash helmets in defiance of the traffic rule by the Federal Road Safety Corps (FRSC), which mandates everybody riding motor cycle to always crash helmet. Though, one may say that the culture of deviance to traffic rules among road users is a factor responsible for the non-compliance by most motor-cyclists because they are willing, they can still manage to buy it but the point we are making here, is that the situation has been further compounded by the sharp inflation in the cost of crash helmets since the implementation of the law in Nigeria.

No doubt, this situation captures the challenges faced by the masses where every law for risk mitigation by the government is always used to take advantage of the poor with the aim of making much profit. The prevailing circumstance in which the cost of purchasing a crash helmet has risen by about 300% has deepened the vulnerability of the motor cyclists. Here, they face risks of possible fatality from accident(s) and also risk of arrest and prosecution by the law enforcement agents for failing to obey the new law.

It is very sad that the government that is enforcing the use of crash helmets has nevertheless failed in its responsibility, to regulate the prices of these helmets. Even, in the leading capitalist nations, the prices of very essential products are still being regulated by government let alone a less capitalist state like Nigeria. We should still acknowledge the efforts made by some state governments to get these helmets for the commercial cyclists but not without political undertone.

Knowing the adverse impact that poor political and economic policies can have on the masses, VCA usually involves empowering the people and alleviating the incidence of impoverishment and poverty among them because they can easily affect "...people's level of vulnerability and the strength of their capacity to resist, cope and recover" (IFRC, 2006). It is against this background that one of the objectives of VCA is to work towards poverty reduction and economic empowerment; and

(e) Aiding development: Another objective of vulnerable and capacity assessment is to engender and promote development in any given community. One of the

reasons is the capability of disaster to wipe out the development that people have laboured for in a given community for several years in hours or even minutes. In order to aid further development, adoption of VCA is targeted towards improved alertness and preparedness of people against any massive losses that hazards or threats may bring into bear, by engaging in such activities like risk education, risk reduction, appreciation of early warnings, disaster mitigation, preparedness, protective actions, to mention a few.
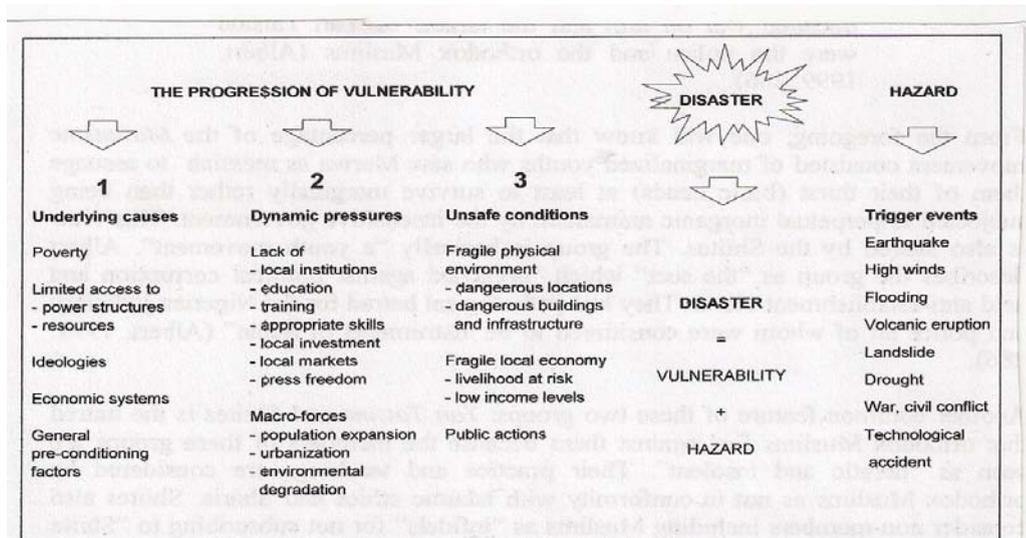
SELF ASSESSMENT EXERCISE

Explain the objectives of vulnerable and capacity assessment as a framework for building the capacity of the masses towards disaster mitigation.

3.3   **Importance of Vulnerable and Capacity Assessment**

a)   Mitigating the impact of hazard: VCA plays great roles in the reduction or mitigation of the impact that incident of hazard or threat can have on people or any community. It creates opportunity for people to participate in disaster management processes, and gain knowledge and transferable skills on ways to manage hazard or threat, so that they can take care of themselves whenever they experience any hazard or attack;

b)   Address of fundamental socio-economic issues: It assists to address issues by drawing the attention of both the ruled and rulers to some issues that can undermine the overall security of any given community. One of the factors that promote vulnerability is poverty, and VCA advocates for drastic poverty reduction, if it cannot be eliminated completely. It is not an exaggeration to contend that it has a tendency of engendering a cycle of vulnerability because "…today's poverty is yesterday's unaddressed vulnerability" (Yamin *et al.*, 2005). What we mean is that if issues of poverty are not adequately addressed it can generate another set of vulnerabilities, which will also lead to another incidence of poverty, as the situation keeps rotating in circular form and culminating in disaster. See **figure 1.1**:

FIGURE 1.1   The Progression of Vulnerability

THE PROGRESSION OF VULNERABILITY

1 Underlying causes	2 Dynamic pressures	3 Unsafe conditions	DISASTER	HAZARD / Trigger events
Poverty	Lack of – local institutions – education – training – appropriate skills – local investment – local markets – press freedom	Fragile physical environment – dangerous locations – dangerous buildings and infrastructure	DISASTER = VULNERABILITY + HAZARD	Earthquake High winds Flooding Volcanic eruption Landslide Drought
Limited access to – power structures – resources				
Ideologies		Fragile local economy – livelihood at risk – low income levels		
Economic systems				
General pre-conditioning factors	Macro-forces – population expansion – urbanization – environmental degradation	Public actions		War, civil conflict Technological accident

Source: ://reliefweb.int/rw/lib.nsf/db900sid/LGEL-5G8F5Q/$file/ifrc-Toolbox-oct96.pdf? openelement.

It is however advisable to call for reforms if there is deficiency in the existing policies by government especially if they fail to take care of the basic needs of the people. This is because the risk that deprivation can pose to the security of any state as evident in the Niger-Delta region of Nigeria is enormous. Successive governments have failed to do enough in addressing the problem of environmental degradation and the agelong deprivation being suffered by the people of this region. It was not surprising that the youth of the area had to resolve to take up arms against the Nigerian government. The situation of militancy, sabotage and hostage-taking in the region has almost reached a point of disaster. We cannot but pray that the current peace-making arrangement including the granting of amnesty to the militants by government would yield the long-desired peace in the region;

c) Early warning mechanism: It can also serve as an early warning mechanism to alert the government or the people on the impeding danger that specific activities may portend to the (entire) security of live and property in the state. As security experts or professionals, we can also perform this function through intelligence reporting. For instance, there is an impending risk to public security where the political elite recruit youths for political thuggery. This is because there is the tendency that some of these recruited youth if dumped by their former patrons or in a situation of the demise of their masters, will become very vulnerable. And their vulnerable state makes them to seek for alternative means to survive, no doubt that many of them become armed robbers, kidnappers, car snatchers, etc.

Early warning can also be applied for private security. Through security education and knowledge of hazard (disaster) mitigation and prevention, people become aware of the risk involved in the specific aspects of their lifestyles or private activities to their personal safety. For instance, many NGOs visit

schools to educate students on the danger of engaging in premarital sex, sharing of sharp objects and unprotected sex. The reason is to alert them on the possible contraction of deadly infections like the HIV-AIDS, so that they can prepare themselves to avoid engaging in such habits. Even, in a situation that such a student wants to engage in sex, he/she is advised to use condom. This process of alertness and advice can constitute early warning;

d) <u>Promotion of development</u>: It helps in the promotion by encouraging further developmental projects and activities among the stakeholders in any community, and increases the consciousness of the people and policy makers on how to achieve further development in their immediate community. It also raises hazard preparedness and disaster mitigation as a way of avoiding disruption of their personal and community development by incidence of threat and disaster.

The issues of development are very strategic to the capacity of communities to manage their security. The costly nature of putting in place various developmental facilities has adversely affected the potentials of several developing or poor countries to develop like their counterparts in Europe and elsewhere. For instance, one cannot imagine how much it will cost Nigeria to install surveillance camera in every nooks and cranny of the country but the truth of the matter is that the resources (human and material) being lost through armed robbery alone is unquantifiable. This view is also shared by Mr. Kofi Annan, the erstwhile Secretary-General of the United Nations (UN), and according to him:

More effective prevention strategies would save not only tens of billions of dollars, but save tens of thousands of lives. (…) Building a culture of prevention is not easy. While the costs of prevention have to be paid in the present, its benefits lie in a distant future. Moreover, the benefits are not tangible; they are the disasters that did NOT happen (Annan, 1999).

In as much as development takes a lot of time to accomplish, there is no amount of money that is too much to protect it and ensure that disaster is prevented from destroying it. For instance, it is very laughable for an individual to use millions of Naira to purchase a car and finds it very difficult to spend little money on the purchase of fire extinguisher to put in his/her. In the case of fire outbreak, the car may likely burn down completely except there is timely and adequate response to quench the fire. Though, this scenario may look like a farce but it is something that happens in Nigeria where poor habits of risk taking has remained prevalent among the people; and

e) <u>Detection of possible threats or hazards</u>: It helps us to gather information on potential security threats through the application of several participatory tools, which will enable us to identify the degree to which each individual is exposed to threats or hazards. For instance, in a family where one of its members is

infected with tuberculosis and the house they are staying is poorly ventilated. Through VCA, professional advice can be timely and adequately provided to reduce the possibility of the disease spreading to other members of the family as well as providing medical countermeasures especially in the treatment of the affected person. The grassroot nature of VCA makes the whole process a very interactive one, so that the public can be encouraged to participate actively in the issues that bother on their own security and that of the community at large.

SELF ASSESSEMENT EXERCISE

Discuss the importance of VCA in disaster mitigation.

4.0   CONCLUSION

The development that took a whole community over fifty years to accomplish can be destroyed within minutes as a result of disaster. Disaster can express itself in natural or human forms. Some natural disasters like flood can wash away most of the social infrastructure in any community, and this phenomenon is capable of distorting the process of development of any community. Even, on domestic front, many people have virtually lost everything they had worked for in their life-time to disasters such as inferno. Vulnerability and capacity assessment involves a process in which sustainable development activities are integrated with disaster management and mitigation practices. It provides a grassroot forum to the public to acquire transferable skills and knowledge about the ways through which they can respond effectively to reduce losses from hazards and attacks.

5.0   SUMMARY

In this unit, we started our study by describing the term vulnerability and capacity assessment. Thereafter, our attention centred on how the objectives of the vulnerability and capacity assessment can help in building the capacity people especially those who are economically vulnerable to discuss aspects of the lives or other things or issues they consider can make them vulnerable to hazards or threats, as we also discussed some of the ways people can take care of themselves when they experience hazards and mitigate the effect that such hazard can have on them. The last but not the least area of discourse in this unit was the importance of this concept, VCA to prevent incidence of disaster. Thank you for your patience.

6.0   TUTOR-MARKED ASIGNMENT

Write a short note on the meaning of vulnerable and capacity assessment, and any four of its objectives.

7.0   REFERENCE AND FURTHER READING

Annan, K. (1999). *Annual Report of the Secretary-General on the Work of the Organization of United Nations*. Document A/54/1. New York: United Nations.

Blaikie P., Cannon, T., Davis, I. & Wisner, B. (1994). *At Risk: Natural Hazards, People's Vulnerability and Disasters*. London: Routledge.

Chambers, R. (1989). Vulnerability: How the Poor Cope. *IDS Bulletin*: 20 (2)

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

 ://reliefweb.int/rw/lib.nsf/db900sid/LGEL-5G8F5Q/$file/ifrc-Toolbox-oct96.pdf?openelement. Retrieved on 20 August 2009.
International Federation of Red Cross and Red Crescent Societies (IFRC). (2006). *An introduction to vulnerability and capacity assessment*. Geneva.

Kuban, R & MacKenzie-Carey, H. (2001). *Community-wide Vulnerability and Capacity Assessment (CVCA)*. Also available on **Error! Hyperlink reference not valid.**. Retrieved on 21 August 2009.

Raphael, B. (1986). *When Disaster Strikes: How Individuals and Communities Cope with Catastrophe*. New York: Basic Books.

United Nations International Strategy for Disaster Reduction (ISDR). (2005). *Reducing Disaster Risk: a challenge for development*. Geneva: ISDR.

Yamin, F., Rahman, A & Huq, S. (2005). Vulnerability, Adaptation and Climate Disasters: A Conceptual Overview. *IDS Bulletin,* 36 (4)

UNIT 3

SIMULATION IN LAW ENFORCEMENT

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 have an 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 traditional Ila-Orangun in present day Osun state, Nigeria, after a series of simulation exercise by the community guards, they discovered that offensive attacks may come from enemies without any prior notice especially in the middle of the night. Therefore, they decided to make a very big hole 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 by enemies' attacks. 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 simulating 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 behaviour 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 behaviour of a system. More practically, simulation can be used to predict (forecast) the future behaviour of a system, and determine what you can do to influence that future behaviour. 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](://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, simulation can be used differently by various professions or for different purposes. But, at the beginning of the 20th century, the 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 malpractices. 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 conduct simulation exercise to put their preparedness to test on how timely and effectively they can respond against any security threats. They act the simulating scripts as if the situation is real. Frankly, it is no exaggeration that Nigeria police lacks absolutely the culture of security simulation. Had the authorities of the nation's police promote regular conduct of simulation exercise, the way the men and officers of the police are being killed on regular basis from attacks in police stations, armed robbers' bullets or any other threats/hazards would have been very minimal. It is not surprising that police personnel always fail to respond very appropriately and effectively to emergency. This shows that their level of preparedness is very far below the average. This is one of the factors responsible for the call being made by concerned citizens, for the introduction of joint patrol that would be composed of members of the police and the armed forces especially the Army.

The growing popularity being enjoyed by computer has led to the use of computer as a platform through which any kind of simulation can be facilitated be it health-care

simulation or military simulation or education simulation or any other forms of simulation. A lot of simulation software has also been invented and it is left for 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, simulation can be used for numerous purposes depending on the problem we aim to unravel and apply solution to.

The complexity of the problem we are working on may require 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) <u>Education and Training Simulation</u>: Security profession requires sufficient mental alertness and physical strength, and that is why it is not everybody that can do a security job. The nature of security profession underscores the need by professionals to always engage themselves in periodic training. For instance, it is very sad to hear such situations where the police pursue armed robbers and fail to pin-down the bandits despite the numerical strength and strategic advantage the police has over them. Someone argues that most times the bandits appear to be more equipped than the police as the reason for 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.

Also, the problem of police teams being overpowered by the sophistication of the weapons that robbers carry can be easily addressed if the men and officers of the police can undergo simulation exercise from time to time. Even, members of every 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, then they can map out strategies to adopt to build their capacity towards preventing the threats from happening or mitigating the effect, that such threats can have on them or their operation 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. Most times, police patrol (rescue) teams are found in the habits of announcing to the robbers of their (the police) coming through their blowing of sirens. Unfortunately, before they could reach the location where the robbery is taking place, the robbers would have laid ambush for them, and within a twinkle of an eye, robbers that are well positioned and equipped with sophisticated riffles, would have decimated the ranks of the police teams(s), a situation which often forces the lucky policemen to retreat, as they always find it difficult to recover promptly due to lack of preparedness in hazard mitigation and strategic planning.

Where security practitioners simulate, their preparedness level in acting against any attack will be very high because you would have projected into the future and identify potential threats or challenges you may encounter in the course of discharging your 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 will be recorded will be minimal. I feel it is more appropriate for the police not to alert the robbers of their coming by the blowing of siren. This is because the daring nature of most armed robbers in the country has made the blowing of siren by law enforcement agents obsolete. They are brave and always willing to challenge the law enforcement agents in gun battles. Strategically, for the fact that the rescue team may 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 where a bank robbery is taking place, and wait for the robbers to come out. The reason for this process is to avoid fatality or high losses of lives especially the civilians that may be hit by 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 of whom should be in plain-cloths, so that they cannot be easily identified by the robbers. And as you may be aware, robbers hit the police easily because they can identify them through their uniform. But, if it is considered that the robbers will do more harm by being allowed to complete their operation before attacking them, may be when sporadic killing of customers or bank staff is noticed, a team of experienced officers and men may be sent in.

Caution should be exercised here, there is a need to equip the policemen and officers with bullet-proof vests because people applying for security jobs not with the ultimate desire to suffer avoidable death. Tear-gas may be useful to make the enemies 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 that the security profession is a very tasking one considering the hazards and work-overload that characterise it. Security personnel work long hours, even sometimes they hardly get time to attend to family issues. It is pertinent for the policy makers to see education simulation as an 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 simulated 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 enemies (terrorists, militants, armed robbers etc), one cannot expect that these trainees should be equipped with live ammunitions because of the risk involved in such action.

It will be irrational to allow the use of dangerous 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, many men and officers of the armed forces lobby to be included on peacekeeping contingent without simulating or being able to build scenarios, which can help in making them aware of the inherent risk involved in undertaking peacekeeping mission in a troubled zone(s), and which can help them prepare psychologically, physically, emotionally and strategically. Many soldiers lost their lives after being trapped 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 real 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. 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 a board" (://en.wikipedia.org/wiki/simulation). We shall discuss this type of simulation extensively subsequently (see military simulation);

(b) Health Care Simulation: The form of simulation is also in security and safety, it affords the 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 so 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 as well, which amounts to between US$37 and US$50 million on annual basis. It is very unfortunately 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 that he/she can hardly survive but the poor handling of the situation always result in recording high rate of avoidable deaths in our hospitals.

It is a very abnormal situation where some patients in teaching hospitals are 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 this 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 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 more importance in making brisk business than saving lives. And the decision

makers that are supposed to caution them are less bothered because they get their treatment abroad, even when they have common headache. It is a spoilt system!

Bringing our attention back to the subject under discourse, health-care simulation has been demonstrating growing relevance in modern medical world. Several medical simulators usually involve connecting computer to a plastic simulation of related anatomy, and some of these simulators can be applied through 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 often been 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, be refined without undergoing the real hostility of warfare. The rationale behind military simulation is to facilitate a process through which we 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 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 real experience of the real players or participants. For instance, those who usually have experience of Play Station (game) especially the soccer, you will notice that each of the players demonstrates the real capacity of the model player(s).

In Play Station 2, the scoring ability of Christiano 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, the fact is that there was 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, 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. Finally, 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 submission 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 the uncertainty that characterises the general affairs including security issues in recent time. For instance, since the end of the Cold War, state actors constitute 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 September 11 2001 terrorist attack in the US has shown the very destructive dimension, which threat emanating from non-state actors has assumed. Prior to that ugly incident, nobody would believe that commercial planes could be used as a weapon 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 the ones 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 mounting 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, is that simulation can be applied in various fields or disciplines and for different purposes. It is against that background, we thought it necessary to discuss some of the basic types of simulation that we can employ in security planning and management in order to safeguard the security of the people. I hope that you have found this unit as interesting as you have expected it to be. Well, if you have any question on any aspect of this unit or the course in general, please feel free to get in touch with your instructional and tutorial facilitator or get in touch with the writer through the coordinator of the course. 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.

UNIT 4

CRIME ANALYSIS: MEANING AND IMPORTANCE IN THREAT MITIGATION

CONTENTS

1.0   INTRODUCTION

Professionally, crime analysis as a subfield in Criminology and Security Studies became popular in the 1960s but some of the attributes of crime analysis could be found in ancient security practice. Due to the growing relevance being enjoyed by information and communication technology, crime analysis in the 1990s underwent a reform and sophistication. There is no doubt that computer revolution has contributed greatly to the advanced state that crime analysis finds itself in recent time. In practical terms, crime analysis is often applied at various levels of law enforcement in any community to have an understanding of the situations of crime and their types as well as ways through which they can be reduced if not eradicated.

In Nigeria, absence of necessary modern technologies has undermined the capacity of law enforcement agencies in the country to conduct effective analysis of crime. It is very pathetic in this age of information and computer revolution to still have a police institution without any viable computing systems to document types of crime in each community, record of arrests made and the profile of arrested people. Notwithstanding, the Nigeria Police still on regular basis analyses incidence of crime through its reports, bulletin and information provided to the media and people in general.

In several countries, civilians who are professionals in the field of security are usually tasked to conduct crime analysis while some other countries leave the job of analysing crime entirely in the hands of the police or any other relevant law enforcement agencies. In most states in the United States, the police usually has special units for crime analysis where officers with expert knowledge of the crime analysis are tasked to analyse crime in their locality from time to time. In this unit, we shall beam our searchlight on the subject- crime analysis, and we shall show its importance to crime prevention and control.

2.0   OBJECTIVES

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

- Define the term crime analysis;

- Explain the importance of crime analysis; and

- Discuss the components of crime analysis.

3.0   MAIN BODY

3.1   Definition of Crime Analysis

Crime analysis can be defined as:

...a law enforcement function that involves systematic analysis for identifying and analyzing patterns and trends in crime and disorder (://en.wikipedia.org/wiki/Crime_Analysis).

...the act of analyzing crime. More specifically, crime analysis is the breaking up of acts committed in violation of laws into their parts to find out their nature and reporting statements of these findings. The objective of most crime analysis is to find meaningful information in vast amounts of data and disseminate this information to officers and investigators in the field to assist in their efforts to apprehend criminals and suppress criminal activity. Assessing crime through analysis also helps in crime prevention efforts. Preventing crime costs less than trying to apprehend criminals after crimes occur (Osborne & Wernicke, 2003: 1).

...the individual or unit in a police department charged with processing data and providing information that the agency can use to reduce, prevent, and solve crime, disorder, and quality of life issues ([://www.macrimeanalysts.com/articles/whatis crimeanalysis.pdf](://www.macrimeanalysts.com/articles/whatiscrimeanalysis.pdf)

...a set of systematic, analytical processes directed at providing timely and pertinent information relative to crime patterns and trend correlations to assist operational and administrative personnel in planning the deployment of resources for the prevention and suppression of criminal activities, aiding the investigative process, and increasing apprehensions and the clearance of cases. Within this context, crime analysis supports a number of department functions including patrol deployment, special operations and tactical units, investigations, planning and research, crime prevention, and administrative services (budgeting and program planning). (Gottlieb, Arenberg, and Singh 1994, 13).

SELF ASSESSMENT EXERCISE

Define the term crime analysis.

3.2   **Importance of Crime Analysis**

i.   Crime analysis can be conducted at various levels (tactical, operational, and strategic). One of its purposes is to assist the law enforcement agents to study crime report, reports concerning the biodata and profiles of those arrested, as well as a comprehensive report of all cases of police interventions aimed at identifying the patterns, frequency level, and trends of crimes in any given community;

ii.   Another purpose of crime analysis is to enable us as security operatives to analyse incidents and types of crime in any given society with the aim of identifying their causes and how frequently they occur. By doing this, we shall be able to predict or forecast the future occurrences of these crimes. For instance, in Nigeria, many security reports and findings have shown that incidences of robbery, burglary and road accidents occur more in the last three months of each year. Whenever we are approaching the last three months of the year, the relevant security authorities usually educate the people about the impeding risk that growing crime rate during that period portend to the community at large.

Apart from raising the consciousness of the people about the growing incidence of hazard and threat with the aim of increasing their preparedness towards crime mitigation, the law enforcement agencies mobilise themselves to combat potential growing crimes and hazards that often characterise the months of October, November and December in Nigeria through effective deployment of relevant tactical and strategic measures. As you may be aware, in Nigeria,

during the "ember period" including September, October, November and December, the Federal Road Safety Corps (FRSC) authorities often mobilise their men and officers to step-up their activities in ensuring strict compliance of road users to the traffic rules with the aim of reducing avoidable accidents on our roads.

iii.   Crime analysis allows for statistical evaluation as well as drawing of data queries or/and maps in analysing the patterns and trends in every location within a country. With the availability of data queries, we shall be able to identify particular criminal activities that are often experienced by each community, so that we can develop mitigation techniques to arrest the situation(s) of crime and criminality.

Through statistical evaluation, we determine numerically the trend and patterns of crime in any society. For instance, statistics have shown that the incidents of rape takes place in quick succession more during festive and celebration periods than any other time. For instance, the incidence of rape is mostly reported in Ijebu-Ode (of Ogun State, South Western Nigeria) during the period of *Oju de Oba* celebration. The celebration event that is usually annually observed among the indigenes of Ijebu-Ode draws people from far and near. Due to the influx of people, situations of crime in the ancient town rapidly increases and rape is usually one of the mostly reported cases of crime that often characterise this festive period.

Perhaps, the incidents of rape increases the risk of spread of sexually transmitted diseases including HIV-AIDS in the country, and it is therefore, germane to increase the presence of law enforcement agents when such a big fiesta is taking place. The use of statistics will also afford us the opportunity to determine whether any particular crime(s) is increasing or reducing. We can also use our findings to compare trends and patterns of crime(s) between two communities or more.

iv.   Crime analysis can also serve the purpose of enabling law enforcement agents to provide valuable and vital information or report about criminal incidents in various communities to the people but also assist law enforcement agents in preparing criminal intelligence for court presentations aimed at prosecuting offenders.

v.   Crime analysis is very essential in determining the socio-demographics of crime. It affords us the opportunity of having a knowledge about social and demographic causes and graphical interpretation of crime in any given locality or society or within the jurisdiction of respective security agencies (Boba, 2005: 6–7).

SELF ASSESSMENT EXERCISE

Explain the importance of Crime Analysis.

3.3   Components of Crime Analysis

In crime analysis, security professionals and law enforcement agents apply various tools that are basic components of crime analysis process, and these include:

3.3.1   Data Mining

Data mining is an essential tool of crime analysis. It can 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 is usually employed in the analysis of crime to have a better understanding of the incidence of crime through the study of pattern and trends of crime with the use of intelligence and information gathered from different sources. In the following unit, we shall be shedding more light on the subject-data mining and its relevance to crime detection and mitigation.

3.3.2   Crime Mapping

Crime mapping is another vital tool being employed by security experts or law enforcement agents to analyse crime in any given community. Crime mapping can be defined as a method:

...used by analysts in law enforcement agencies to map, visualize, and analyze crime incident patterns. It is a key component of crime analyse (**Error! Hyperlink reference not valid.**).

It can also be defined as:

...the direct application that comes from considering the inherent geography in crime (://www.jdi.ucl.ac.uk/crime_mapping/index.php).

Crime mapping assists us as security practitioners to have a clearer picture on the patterns and trends of crime in any community with the aim of arrival at decisions that are effective in developing strategies and mitigation interventions for crime control.

3.3.2.1 Elements of Crime mapping

Crime mapping is also essential to tactical analysis necessary for crime forecasting and geographic profiling. In forecasting crime, we predict the occurrence of a particular crime type or another in any given place through the available data we have been able to gather through the process of crime mapping.

For instance, we can forecast that there is high probability that most of the youths used for political thuggery who are equipped with dangerous weapons by some political elite will use the weapons to commit different types of crime in the society, and if their nefarious activities and those of their patrons are not effectively checked, they can become menace to the society at large. It is no news in Nigeria that many former political thugs, after being dumped by their patrons, are using the weapons given to them by those patrons to perpetrate various forms of crime including armed robbery and kidnapping.

Geographic Information Systems (GIS) is a very vital component of crime mapping, which assist crime analysts to locate hot spots or locations where particular crime(s) often take place (Chainey & Ratcliffe, 2005). In crime mapping, we may deploy GIS to develop datasets like census demographics that are essential to locating spots where specific crimes are frequently experienced. With the use of GIS in crime mapping, security practitioners or law enforcement agents do identify where emergency operations and interventions are most needed. The elements of crime mapping include the following:

i.   The use of sophisticated information gathering systems for emergency response: In advanced countries, the law enforcement agencies especially the Police are equipped with comprehensive gazetteers of addresses and locations through computer mapping. The application of computer mapping assists law enforcement agents to identify where an emergency response of the security officers is being sought. Apart from making it easier for the emergency security officers to identify the location that experiences attack or security threat, it also enhances the capacity of the law enforcement agents to prepare against any geographic impediments that topography of the affected area may pose to their intervention.

For instance, in many poorly planned urban centres in Nigeria, the Fire Fighters often encounter mammoth challenge whenever they are responding to emergency call resulting from an outbreak of inferno in any location. It is not all the time that these fire fighters intervene too late to combat the inferno but many of these affected places impede easy access due to the disgusting way people put up their structures such that the fire fighting vehicles will find it extremely difficult to reach the affected place.

However, a visit to Ooje and Bere in the ancient city of Ibadan (Oyo State, Nigeria) will marvel any security-conscious person(s) owing to very abnormal

way buildings were erected such that if there is any outbreak of fire in a house, there is high possibility that the inferno will spread to some other houses. Modern technology has enhanced the capacity of most communities in the world towards crime mitigation. For instance, the introduction of mobile computing with global positioning system (GPS) technologies has made it very easy for any community to detect any incidence of vandalism;

ii. Information Systems and Crime Alert: Resulting from the inability of the law enforcement agents especially the Police to have enough personnel that will cover all nooks and crannies of any community or country at all time, the use of information technology is overlooked. In many developing countries like Nigeria, the number of police personnel is very inadequate to provide any meaningful security to the country as a whole. In addition, the police personnel are poorly motivated and trained, as they have become pawns in the hands of corrupt political elite. It is not surprising that many policemen and officers have been accused to be anti-people and unprofessional, many of whom have forgotten that their main objective is to protect the lives and property of the masses rather than only the rich men.

In as much as police patrol cannot cover everywhere at the same time, the use of the COMPSTAT process using crime mapping can be very helpful to the Police to have a better understanding and adequate information about happenings on the streets. This will also assist them to identify where the police authorities can mobilise the presence of their men for crime prevention and mitigation;

iii. Identification of Crime hotspots: The use of crime mapping through installation of security gadgets like Closed Circuit Televisions (CCTVs) and Secret Cameras can also be strategically helpful in combating criminal activities in any community. The use of CCTVs or secret cameras can help us to monitor the activities and movement of people in any location, and enable us to have the opportunity of detecting any occurrence of crime as well as the location where any criminal activity is taking place with the aim of improving our capacity to respond timely and adequately in arresting the culprits or offenders;

iv. Pattern Analysis: Crime mapping enables us to have a clearer picture of the patterns of criminal activities that are experienced in our local community. Thus, through it, we have a better understanding of crime distribution, and with the use of crime maps and other information on housing, demography etc, we shall be able to create a strategic framework to prevent or/and mitigate crime in our neighbourhoods;

v. Geographic Profiling: In crime mapping, the application of geographic profiling enables the law enforcement agents to identify the most probable residential locations that (notorious) criminals live. In major cities of Nigeria, there are some locations that are marked as the havens of dangerous criminals

229

in the country, and law enforcement agents patrol comb those areas from time to time. In Lagos, places like Akala in Mushin, Ajegunle, Okokomaiko. Iba, Ijora-Badia etc are mapped by law enforcement agents as some of the most probable places where most criminals live;

vi.   Assessing the impact of existing crime reduction approaches: Crime mapping can also help us to evaluate the impact of various crime mitigation techniques we have put in place to combat incidence of crime. It will enable us to identify those of such measures that have actually worked to reduce or curb the incidence of crime (as well as which types of crime they have worked to mitigate) and those other crime reduction measures that have failed to work; and

vii.   The use of maps to communicate to the Public on crime situations: In some advanced countries like the United Kingdom, maps are used in form of media to inform the people about crime situations and crime types that exist in their various places through crime statistics that is transmitted on the internet. This will assist the people to have up-to-date reports concerning amount criminal incidents being recorded in their localities and elsewhere. It will afford the opportunity to know if the criminal activities they experience in their areas are increasing or reducing.

3.3.3 Statistics

Statistics is another component of crime analysis. It is a vital tool of numerically determining the patterns and trends of crime in any community or in comparing the crime situations between two or more communities. Meanwhile, let us quickly define the term statistics but before we undergo the conceptual task, it is important to note that statistics can also be described as an academic discipline rather than only as a set of methods for scientific inquiry and evaluation of data. Here, we refer to statistics as a method through which we analyse crime. Thus, statistics can be described as:

...application of methods to collect, analyze and interpret data. Modern statistical methods involve the design and analysis of experiments and surveys, the quantification of biological, social and scientific phenomenon and the application of statistical principles to understand more about the world around us. Since data are used in most areas of human endeavour, the theory and methods of modern statistics have been applied to a wide variety of fields (://statistics.unl.edu/whatis.shtml*).*

In crime analysis, statistics plays a very important role. It enables security practitioners to put observable crime data to scientific testing through the processes of data collection, analysis and interpretation with a view to solving any problem of crime or criminal investigation. A crime analyst is supposed a good knowledge of statistics to be able to function well professionally. Apart from problem-solving objectives, the use of statistics in crime analysis assists the public to know the crime

situations in their various domains as well as knowing the major threats to their security.

As reiterated earlier, some countries like the UK ensure that people have access to statistical details of crime situations in their local environments, which the law enforcement agents often place on the internet. Through this information, people will be able to know if crime is actually increasing or reducing as well as know types of major crime that frequently occur in their neighbourhood. In having access to all this information, the level of preparedness of the people towards the mitigation of such crimes will be improved. Similarly, by identifying the level of vulnerability of any community to any crimes, it will afford the law enforcement agents the opportunity to prepare themselves towards capacity building for crime mitigation.

3.3.4 Critical Thinking

Critical thinking is an essential component of crime analysis. The subject of criminal investigation and other types of investigation require that security practitioners or law enforcement agents need to carefully interpret the information he/she has gathered for his/her investigation. Here, we consider the logic in response of the suspect in the course of interrogation, evidence sources or materials, contextualisation of issues, observable facts, and consistency of the answers given by the suspects during interrogation session(s) before we come to our judgement about the innocence or culpability of the suspect(s) or persons under investigation in connection with a crime perpetrated.

Now, how do you define the term critical thinking? The available definitions of critical thinking as a concept are many but we shall be considering some of these definitions in our conceptual description of the term. Therefore, critical thinking can be described as:

...skilled, active, interpretation and evaluation of observations, communications, information, and argumentation (Fisher & Scriven, 1997: 20).

Critical thinking is assumed to be the purposeful and reflective judgement about what to believe or what to do in response to observation, experience, verbal or written expressions, or arguments. Critical thinking may involve determining the meaning and significance of what is observed or expressed, or, concerning a given inference or argument, determining whether there is adequate justification to accept the conclusion as true (://en.wikipedia.org/wiki/Critical_thinking).

In security profession we face huge challenge from attempting to make rational and logical conclusions and decisions about issues and subjects of investigation. It is incumbent on every conscientious security practitioner or law enforcement to validate the information at his/her disposal when carrying-out a criminal investigation, so that innocent persons will not be punished. Many people have accused the Nigeria Police of poor credentials particularly in the area of investigation. The reason is not far-

fetched, most policemen and officers lack good knowledge of critical thinking, which is an important element of crime analysis.

Many times, law enforcement agents are accused of acting the scripts of the plaintiffs without verifying the reliability of the accusations levelled against the suspects before they conclude on the suspects' culpability of the alleged crime. For instance, there was a case of a man who reported to the police that he was suspecting that his younger brother had become a criminal owing to the type of friends he was keeping. Swiftly, the police acted on the information given to it and a search was conducted on the suspect's premise. In the process, some guns were found, and consequently the suspect and his friends were arrested.

Sadly, rather than employing critical thinking in the analysis of the alleged crime, the suspects were shot dead by the police. Here, the concerned policemen apart from disobeying the law which says a suspect cannot be said to be guilty of a crime (an offence) until proved to be guilty by the competent court, but also failed to apply critical thinking in analysing the alleged crime. By using critical thinking, they should have carefully put the information supplied to them by the chief suspect's elder brother into analytic and logic validation to determine the accuracy, credibility and precision of the allegation (information) as well as its relevance to truth before coming into judgement on whether the accused were actually culpable of armed robbery or it was a case of a set-up. Due to non-deployment of critical thinking by law enforcement agents, many innocent people have hastily been made to undergo some punishment for the crimes they did not actually commit.

SELF ASSESSMENT EXERCISE

Discuss the components of crime analysis.

4.0   CONCLUSION

Crime analysis remains a vital tool of security management. It helps law enforcement agents especially the police to have a good understanding and knowledge of the patterns and trends of crime within their jurisdiction. It also assists the law enforcement agents to mobilise their resources more productively for effective crime management and enhances their capacity in identifying and arresting the crime suspects. In recent time, the use of spatial data analysis is gaining growing relevance in crime mapping, assisting the law enforcement agents to study crime data with a view to have a greater understanding of why crime is occurring rather than focusing only on where crime occurs.

By and large, crime mapping is an essential component of crime analysis, as it can also be applied for research purposes. It can assist us to have a greater knowledge of the patterns of incarceration and recidivism, target resources and programmes, crime prevention evaluation etc. The other components of crime analysis including data mining, statistics and critical thinking are also germane not only to the analysis of

crime situations but also to vulnerability and capacity assessment through which we can develop strategies and measures towards crime prevention and reduction.

5.0   SUMMARY

In this unit, our subject of discourse was crime analysis and how it can contribute to the prevention and mitigation of crime. We began our lesson by explain the conceptual meaning of the term crime analysis. Thereafter, we focussed on the importance of crime to crime prevention and mitigation. The third area of inquiry was the explanation of the basic components of crime analysis including data mining, crime mapping (and its elements), statistics and critical thinking.

6.0   TUTOR-MARKED ASSIGNMENT

Define crime analysis and explain any four its components.

7.0   REFERENCES AND FURTHER READING

Boba, R. (2005). *Crime Analysis and Crime Mapping*. Thousand Oaks, CA: Sage Publications.

Chainey, S. Ratcliffe, J. (2005). *GIS and Crime Mapping*. John Wiley & Sons. ISBN: 0470860987.

Fisher, A. & Scriven, M. (1997). *Critical Thinking: Its Definition and Assessment.* Norwich: : Center for Research in Critical Thinking.

Gottlieb, S.L., Arenberg, S., and Singh, R. (1994). *Crime Analysis: From First Report to Final Arrest.* Montclair, CA: Alpha Publishing.

Osborne, D. & Wernicke, S. (2003). *Introduction to Crime Analysis: Basic Resources for Criminal Justice Practice*. New York: The Haworth Press, Inc.

://en.wikipedia.org/wiki/Crime_Analysis. Retrieved on 3 October, 2009.

://en.wikipedia.org/wiki/Crime_mapping. Retrieved on 3 October, 2009.

://en.wikipedia.org/wiki/Data_mining. Retrieved on 28 September, 2009.

://statistics.unl.edu/whatis.shtml. Retrieved on 5 October, 2009.

://www.jdi.ucl.ac.uk/crime_mapping/index.php. Retrieved on 5 October, 2009.

://www.macrimeanalysts.com/articles/whatiscrimeanalysis.pdf. Retrieved on 9 October, 2009.

://www.tempe.gov/CAU/about_ca.htm. Retrieved on 4 October, 2009.

UNIT 5

APPLYING DATA MINING AND AUTOMATED DATA ANALYSIS FOR CRIME MANAGEMENT

CONTENTS

1.0   INTRODUCTION

In this unit, we shall beam our search light on the subject, data mining and automated 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 they 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. You will find this unit intellectually rewarding. Meanwhile, in the following segment of this unit, we shall quickly go through the 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 section of this unit, data mining and automated data analysis are inter-related as the 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.

These two concepts can be less effective or absolutely defective, if we fail to understand effectively 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). One of the major features of Social Sciences and other related fields is the absence of universal definition of any term 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.

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

practice, such as marketing, surveillance, fraud detection and scientific discovery (://en.wikipedia.org/wiki/Data_mining).

Data mining can also make 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. It 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 subject can be 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, then we may decide to probe into his/her various contacts or 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 popular among public security practitioners like the Police and intelligence agencies.

Meanwhile, in Nigeria, the 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. The existence of a central information system will enable all its offices to access and make informative 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 state governors in the country to call for the 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 the

Nigeria Police fails to keep proper records 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 the course of investigation, we may identify other people whose presence will be required to provide 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 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 beam our searchlight to know 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 have such big money 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 on our mind to be subjected to further scrutiny.

Thereafter, the suspected persons will become our subjects (those we investigate) and we conduct further search on their activities and relationships. 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 will 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 the effective usage of these two concepts: data mining and automated data analysis.

a) <u>Collection and Processing of Data</u>: 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 have in our minds before we set out for the gathering of data, what we seek to achieve in our analysis, so that we will be able to conclude appropriately well 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. The process is 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, then 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 positives 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 of searches, 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. 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 which 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 to crime management.

6.0   TUTOR-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

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.

://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/data mining.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.