PROFESSIONALISM IN SECURITY AND LAW ENFORCEMENT

INTEGRITY STANDARDS FOR SECURITY ENFORCEMENT EMPLOYEES OPERATING IN DEMOCRATIC ENVIRONMENT

Barrister Adebayo Akinade dfisn & Ade Ogidan fisn

ABSTRACT

There are many issues facing the operations of today's law enforcement officers in the country. Some include the use of excessive force, sometimes deadly; corruption; noncompliance with operational code of ethics; and violation of human rights, among others. Irrespective of these, there is code of ethics guiding all employees within the security system. All law enforcement agencies throughout the country should be required to ensure that their officers adopt the code of ethics as part of their policies and procedures. Each department should make it mandatory for their respective employees to know, as a matter of training, what the code of ethics document represents. The departments should hold annual events, where officers renew their adherence to the code of ethics and oath of office, to usher in a new regime of acceptable professionalism in law enforcement, under the current democratic dispensation.

INTRODUCTION

Democracy is a system of governance where the power originates from the people, through free and fair elections. Public authorities are representatives of the people they serve and their wishes. They respect the principles of democracy.

In a democratic system, there exists three powers-- the legislative, the executive and the judiciary and each plays distinct roles, with defined abilities to check the powers of the other. They exercise the power vested in them by the people for the good of the people.

Table 2: The Role of the Three Arms of Government

Power	Role
Legislative	Proposes, drafts, enacts, amends, and repeals laws. Oversees the activity of the executive.
Executive	Daily administration of the state, executes and enforces the law.
Judiciary	Interprets and applies the law.

Position of Security Law Enforcement Agencies within a Democratic System

The law enforcement agencies are part of the executive power. They are empowered by the people through the executive to maintain order, stability and security. They have to apply the laws enacted by the legislative power on behalf of the people, for the good of the people. They support the judiciary in its mission but cannot make judgments in a judicial context.

Core Functions of the Security Agencies are:

- Prevention of crime
- Detection of crime
- Crisis management and emergency measures
- Maintenance of public order, peace and tranquility
- Provision of assistance to the public

Security Agencies: Principles in Democratic Environment

I. Objectives of Security Agencies in Democratic Environment

The security agencies are the most visible manifestation of government authority. Their main duties are to:

- maintain public tranquility and law and order;
- protect and respect the individual's fundamental rights and freedoms;
- prevent and combat crime; and to
- provide assistance and services to the public.

Security officers will enhance the legitimacy of the State by responding to public needs and expectations; and using the authority of the State in the people's interest.

II. Upholding the Rule of Law

While pursuing these objectives, the law enforcement agencies must:

- Operate in accordance with the domestic law and the international law enforcement standards accepted by the Organisation for Security and Co-operation in Europe (OSCE) participating States; and
- demonstrate commitment to the rule of law in practice.

Legislation and written policies governing the law enforcement agencies should be:

- clear;
- precise; and also
- accessible to the public.

III. Security Personnel: Ethics and Human Rights

In order to live up to the public's trust, the law enforcement agencies must adhere to a code of professional conduct and demonstrate:

- professionalism; and
- integrity.

This code should reflect the highest ethical values, expressed in:

- Prohibitions; and
- imperatives of law enforcement work.

The law enforcement agencies have particular powers to:

- temporarily deprive people of their freedom;
- limit the full enjoyment of their rights; and,
- in extreme circumstances, to use even lethal force.

Therefore, law enforcement officers must perform their duties in accordance with:

- universally agreed standards of human rights; and
- civil and political rights.

Protection and preservation of life must be their highest priority.

Key Principles of Security Personnel in a Democratic Environment

The key principles of security personnel in a democratic environment are:

i. Upholding the rule of law

In a democratic context, all the citizens, including those who are working in the legislative, executive and judicial branches, are equally bound and protected by the law. Everyone, including the security agencies, must decide and act on the basis of, and in accordance with, existing laws, regulations and the legally binding human rights principles.

ii. Public Service

The mission and functions of the police and law enforcement agencies must strive to respond to the security needs of all groups of citizens.

iii. Integrity

In the security context, at the organisational level, integrity signifies that the law enforcement organisation has established and operates in line with ethical values. More specifically, police integrity entails that police work is steered by a core set of clearly defined ethical values such as impartiality, fairness, equality, justice, honesty and respect for human rights. Integrity should be promoted by the security organisations through all their administrative levels. At the individual level, security officers uphold the principle of integrity when they align their behaviour with the ethical values set by their organisation.

iv. Accountability

Accountability means that the security agencies are responsible for their actions and decisions. Hence, security officers and organisations answer for their acts and can be held accountable for them (e.g. by parliamentary oversight, review and monitoring by independent oversight bodies such as ombudsman-institutions, elections, sanctions in case of an arbitrary decisions).

v. Transparency

Transparency signifies that policies, laws, budgets, and information on decisions and activities of the police are easily accessible to the public. Information should be relevant, of good quality and provided in a timely manner. Lack of such information hinders accountability because the citizens will not be able to evaluate and scrutinize the way the police exercise the special powers vested in them by the people of the democratic State.

Due to the nature of the police and law enforcement mission and functions, it may be necessary to have a certain level of secrecy as regards some aspects of their day-to-day-operations.

vi. Representativeness

The security workforce reflects the social composition of the society where it operates. Access to the security is not restricted to individuals belonging to a specific group (e.g. ethnic majority group) or having a particular quality (e.g. gender, level of education) and efforts are made to integrate and to maintain, as far as possible, different groups of the population in the police force.

vii. Effectiveness and Efficiency

A security agency is effective when it is able to perform its core functions or roles and accomplish its goals. The agency is efficient when resources (time, budget, human, and material resources) are optimally allocated for the performance of functions and achievement of goals.

The principle of efficiency does not operate in a vacuum. It has to be considered in the wider context of the other democratic policing principles. In considering the optimal way to accomplish a police function, law enforcement officers and their organisations in general have to ensure that the other key principles of law enforcement, such as integrity, rule of law and accountability are
not compromised.

Principles of Security Enforcement in a Democratic Environment

In order to properly exercise their functions or roles in a democratic society, the security agencies must uphold certain principles.
There are eight essential principles of Law enforcement in a Democratic Environment:

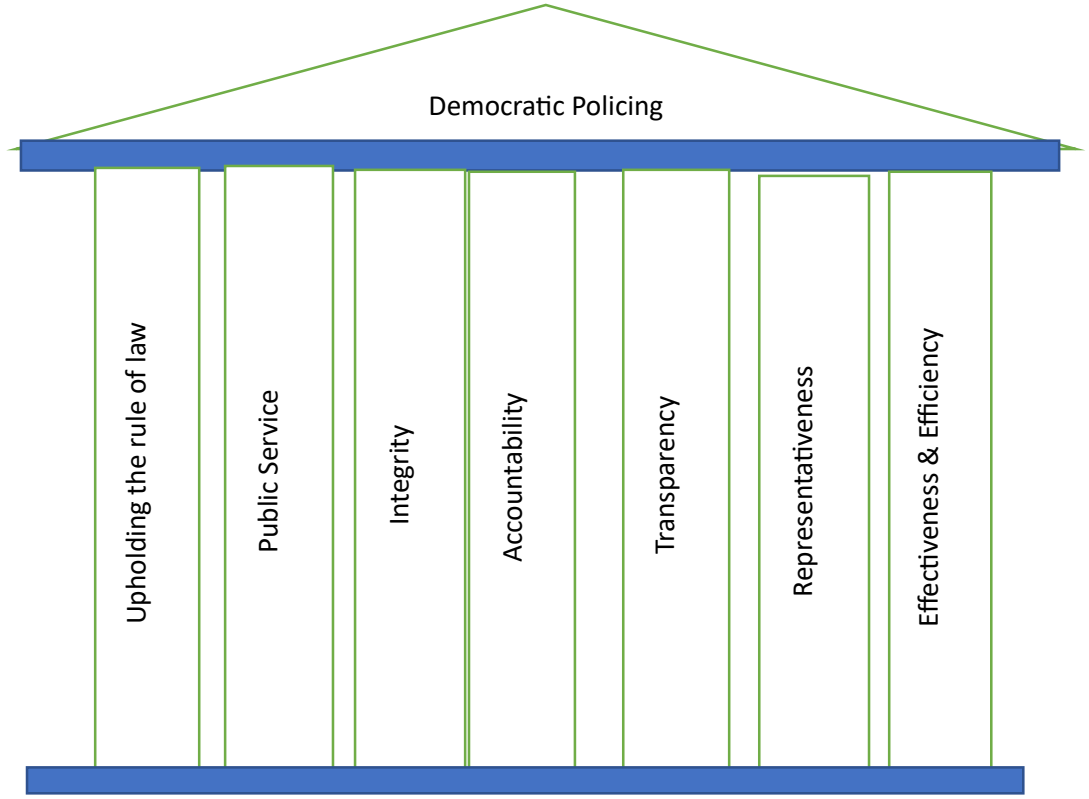


Fig. 4: Essential Principles of Security Enforcement in a Democratic Environment

Integrity and Security Enforcement

The definitions of integrity entail two elements. The first one is what is right in respect of ethical values, moral principles and wisdom. The second one is what you do, that is, your actions and behaviour. Integrity is having the inner personal strength and courage to always link the two, even in difficult situations, despite having no advantage from it or even risk being disadvantaged by it, when others want or expect you to behave differently: align your **behaviour** with ethical **values**, **do** what is right. Integrity is the principle of consistently behaving in accordance with ethical values.

There is the need to know the basic concepts of the following related terms:

i. **Ethics** is a set of values and norms commonly accepted in a society or profession as right (i.e. police ethics). A person who has integrity should have values that are consistent with ethics and behave ethically.

ii. **Human rights** are related to integrity in two ways. Firstly, they include the right to life, fair treatment, equality, which are values that are considered universal and should guide everyone's actions. Secondly, human rights are also part of international and national law, and respecting the law is one behavioural characteristic of people who have integrity.

Essentially, human rights are the basic rights and freedoms to which all humans are entitled to, often held to include the right to life and liberty; freedom of thought and expression; and equality before the law. They are related to integrity in two ways. Also, human rights are values that are considered universal and should guide everyone's actions. But human rights are also part of international and national law and respecting the law is one behavioural characteristic of persons who have integrity.

iii. **Honesty** is one value and a behavioural characteristic of integrity. A person who has integrity should value honesty and behave honestly. Honesty is the quality of being fair and truthful. It is one behavioural characteristic of integrity.

iv. **Corruption** is one specific type of violation of moral norms and values, along with other types of crimes, misconduct or unethical behaviour. It is one manifestation of a lack of integrity. Corruption is the abuse of public office for private gain, whether material or non-material. It is one manifestation of lack of integrity.

v. **Organisational integrity** exists when an organisation operates in line with a set of clearly defined ethical values. Values can be defined for instance in the organisation's vision, mission and code of ethics. These values are integrated into internal processes, by employees and into the organisation's interaction with its environment. The organisation ensures respect and visibility of these values by appropriate communication, leadership, strategies, policies, rules, control, accountability and transparency.

"Organisational integrity is more than just preventing corruption or having a written code of conduct. It is when an organisation's operational systems, corruption prevention strategies and ethical standards are fully integrated to achieve its purpose. Everyone has a personal set of ethical values and the vast majority of public officials and staff have positive ethics. But personal integrity is not really the focus here. With organisational integrity, the focus is on forming an underlying set of values for your organisation as a whole and integrating them with tried-and-true corruption prevention strategies and, in fact, with all the workings of your organisation."

vi. **Integrity** is the principle of consistently behaving in accordance with ethical values. Individual integrity is the moral strength of aligning behaviour with ethical values.

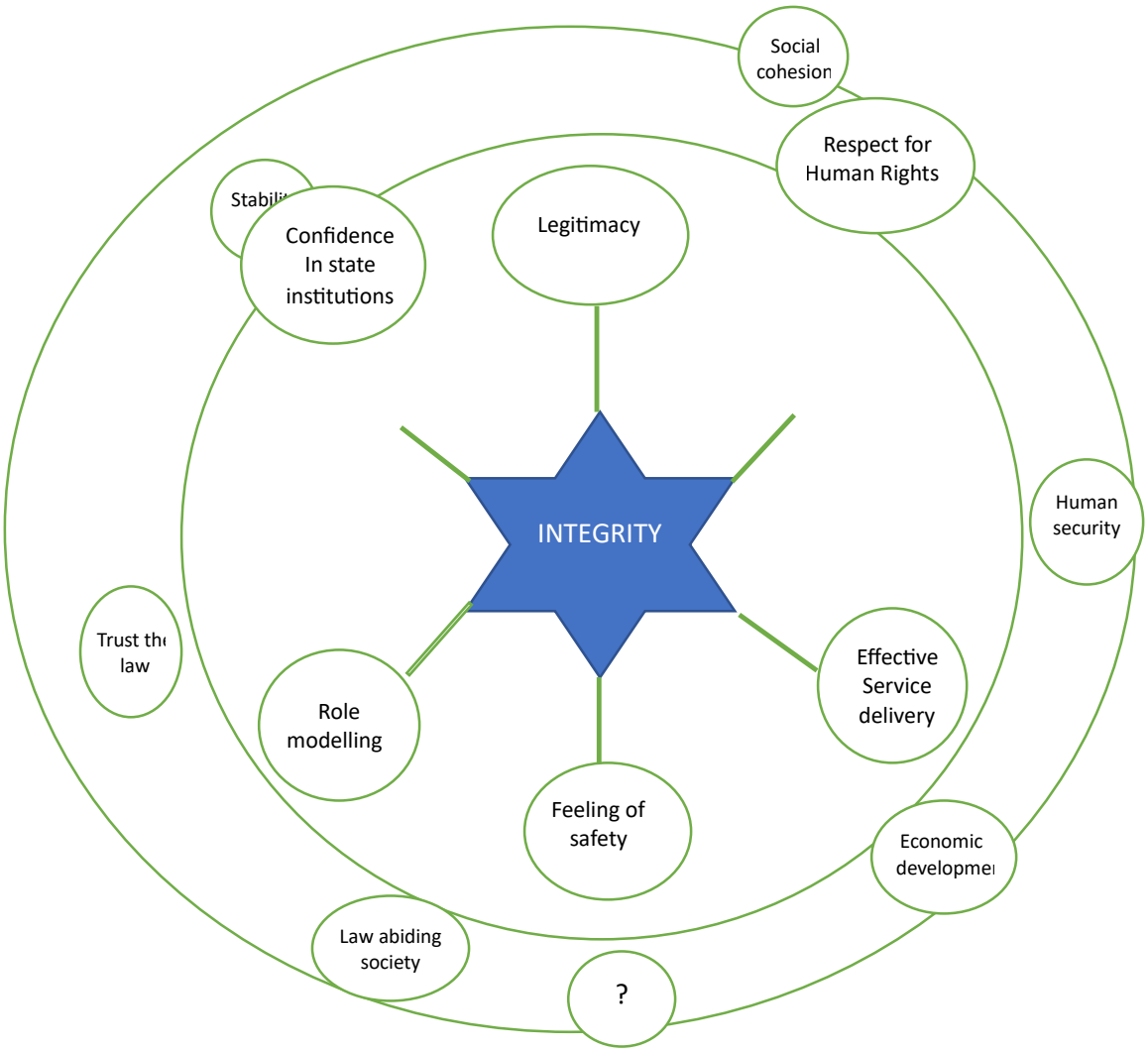


Fig. 5: Benefits of Police Integrity for the Society

The importances of law enforcement integrity are:

Respect for Human Rights – The police and law enforcement agencies are entrusted with special powers such as arrest, detention, coercion and use of force. If not used with the highest levels of restraint and integrity, these powers might easily lead to human rights violations.

Legitimacy – In a democratic system, it is crucial that state institutions enjoy legitimacy, i.e. that people perceive public authorities as representatives of public will. The legitimacy of the police and law enforcement agencies is strongly enhanced if the public recognizes that the police powers are used to serve the public with integrity, impartiality and fairness.

Effective Service Delivery – Modern societies are increasingly relying on public cooperation for the successful performance of law enforcement mandate. Law enforcement integrity is essential to create trust between the public and the law enforcement agencies, as trust enhances citizens' inclination to cooperate with the law enforcement agencies and provide useful information in support of crime prevention and repression.

Feeling of Safety – When people believe that law enforcement agencies are committed to serve and protect everyone equally, they tend to feel safer in their preoccupations.

Role Modelling – The law enforcement agencies are the state agencies responsible for ensuring the respect of the law and maintaining the moral order in the society. By displaying integrity in their own work, police officers act as role models for other citizens and promote respect for the law and ethics.

Confidence in State institutions – Law enforcement officers are the most visible representatives of the State. Their image reflects on the image of the State and confidence in them influences the public's confidence in the other State's institutions.

THE SECURITY AGENCIES AND THE CRIMINAL JUSTICE SYSTEM

- There shall be a clear distinction between the role of the law enforcement agencies and the the judiciary cum the correctional system. The law enforcement agencies shall not have any controlling functions over these bodies.

- The law enforcement agencies must strictly respect the independence and impartiality of judges. In particular, the law enforcement agencies shall neither raise objections to legitimate judgments or judicial decisions, nor hinder their execution.

- The law enforcement agencies shall, as a general rule, have no judicial functions. Any delegation of judicial powers to the police shall be limited and in accordance with the law. It must always be possible to challenge any act, decision or omission affecting individual rights by the police before the judicial authorities.

There shall be functional and appropriate co-operation between the law enforcement agencies and the public prosecution. In countries where the police are placed under the authority of the public prosecution or the investigating judge, the police shall receive clear instructions as to the priorities governing crime investigation policy and the progress of criminal investigation in individual cases. The police should keep the superior crime investigation authorities informed of the implementation of their instructions. The development of criminal cases should be reported regularly.

- The police shall respect the role of defence lawyers in the criminal justice process and, whenever appropriate, assist in ensuring the right of access to legal assistance, in particular with regard to persons deprived of their liberty.

- The police shall not take the role of prison staff, except in cases of emergency.

- The police shall be organised with a view to earning public respect as professional upholders of the law and providers of services to the public.

- The police shall enjoy sufficient operational independence from other state bodies in carrying out given tasks, for which it should be fully accountable.

- The police shall be organised in a way that promotes good police/public relations and, where appropriate, effective co-operation with other agencies, local communities, non-governmental organisations and other representatives of the public, including ethnic minority groups.

- Police organisations shall be ready to give objective information on their activities to the public, without disclosing confidential information. Professional guidelines for media contacts shall be established.

- The police organisation shall contain efficient measures to ensure the integrity and proper performance of

police staff in particular, to guarantee respect for individuals' fundamental rights and freedoms as enshrined, notably, in the European Convention on Human Rights.

Policing as a Public Service

1. The main duties of the police are to maintain public tranquility, law and order; to protect the individual's fundamental rights and freedoms – particularly life; to prevent and detect crime; to reduce fear; and to provide assistance and services to the public.

   Progress towards democratic policing is made when there is a shift "from a control-oriented approach to a more service-oriented approach", where the primary concern of law enforcement remains focused on proactive crime prevention.

2. Democratic police develop and implement their activities according to the needs of the public and the State and emphasise assistance to those members of the community in need of immediate help.

The police must be responsive to the community as a whole and strive to deliver their services promptly and in an equal and unbiased manner. Through their activities, the police should be part of society's common efforts to promote legal protection and sense of security.

1. Upon request, the police shall assist other public institutions in performing their services when prescribed by the law. When intervening in conflicts, the police must be guided by the principle that "everyone shall be subject to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the right and freedom of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society". The police can therefore, be considered the gatekeepers of equality, integration and cohesion in a time of rapidly changing composition of the population in most major cities.

2. When problems are brought to the police to be resolved the response would indicate the extent to which democratic policing practices have been adopted.

3. The police will enhance the legitimacy of the State if they demonstrate in their daily work that they are responsive to public needs and expectations, and they use the authority of the State in the people's interest. If the police carry out their responsibilities in a way that reflects democratic values, the cause of democracy and the legitimacy of the State are advanced.

4. Public trust and confidence in the police are prerequisites for effective policing. Without this trust, the public will not be willing to report crimes and provide the police with the information needed to work successfully.

5. Furthermore, democratic policing requires that the police simultaneously stand outside of politics and protect democratic political activities and processes (e.g. freedom of speech, public gatherings, and demonstrations). Otherwise, democracy will be threatened.

RECRUITMENT AND REPRESENTATION

1. The composition of the police – at local, regional and national levels and including senior as well as junior ranks, and also civilian personnel – should reflect the diversity of the population.

The public image of the police as an ethnically representative body needs to be actively promoted. Equitable representation of minorities in the police organisation is important for several reasons:

a) As an indicator that members of all ethnic groups have equal opportunity as individuals to join and progress in careers in the police;

b) As a way of promoting integration of minorities through their participation in the public life of the state and its institutions;
c) As a way of providing the police organisation internally with a range of knowledge and skills (including language skills) that are required for working in an ethnically diverse community;

d) As a means of helping police to build relationships externally with minority communities based on effective communication, co-operation and mutual confidence.

Security Enforcement Code of Ethics and the Use of Authority

The law gives police extraordinary powers and, at the same time, circumscribes those powers in a manner that ensures that they are not abused. This form of expression of the doctrine of the separation of powers not only ensures that power is not abused but also has the consequence of enhancing the reputation of the police as a fair-dealing body. It is the very values that underline police governance that ensure it. In order to illustrate the relevance of the study of ethics, the use of authority in the criminal justice system, a number of specific codes of ethics, ethical problems and issues that might arise for professionals in the criminal justice system are set out in the subsequent sections. These problems and issues might, for example, be concerned with how to exercise authority and how to deal with conflicts, or with ethical issues confined within one particular part of the system, such as juvenile justice.

Essentially, it may be considered that questions of professional ethics would be of greater concern to members of the liberal professions than to public servants such as the police. However, professional ethics can also be important in the police profession, by its very nature and the conditions in which its members fulfil their function. A police officer has extensive powers conferred on him, and he exercises these powers in the context of professional duties, hence the necessity of an internalized ethic, which would certainly gain from a codification. Through such a code of professional ethics, the legal provisions normally contained in the general regulations for public servants are raised to the level of professional moral imperative. The code of professional ethics is then seen as a means of transmitting a standard, the purpose of which would be to induce police officers to adhere to a system of values combining professional efficiency with respect for basic liberties.

Primary Responsibilities of Security Enforcement Officers

A security enforcement officer acts as an official representative of government. who is required and trusted to work within the law. The officers' powers and duties are conferred by statute. The fundamental duties of a police officer include serving the community; safeguarding lives and property; protecting the innocent; keeping the peace; and ensuring the rights of all to liberty, equality and justice.

Performance of the Duties of Law Enforcement Officer

A law enforcement officer shall perform all duties impartially, without favour or affection or ill will and without regard to status, sex, race, religion, political belief or aspiration. All citizens will be treated equally with courtesy, consideration and dignity. Officers will never allow personal feelings, animosities or friendships to influence official conduct. Laws will be enforced appropriately and courteously and in carrying out their responsibilities, officers will strive to obtain maximum cooperation from the public. They will conduct themselves in appearance and deportment in such a manner as to inspire confidence and respect for the position of public trust they hold.

DISCRETION

A security enforcement officer will use responsibly the discretion vested in the position and exercise it within the law. The principle of reasonableness will guide the officer's determinations and the officer will consider all surrounding circumstances in determining whether any legal action shall be taken.

Consistent and appropriate use of discretion, based on professional policing competence, will do much to preserve good relationships and retain the confidence of the public. There can be difficulty in choosing between conflicting courses of action. It is important to remember that a timely word of advice rather that arrest – which may be correct in appropriate circumstances – can be a more effective means of achieving a desired end.

USE OF FORCE

A security enforcement officer will never employ unnecessary force or violence and will use only such force in the discharge of duty reasonably in all circumstances. Force should be used only with the greatest restraint and only after discussion, negotiation and persuasion have been found to be inappropriate or ineffective. While the use of force is occasionally unavoidable, every police officer will only use the minimal level of force that is necessary and never engage in cruel, degrading or inhuman treatment of any person.

CONFIDENTIALITY

Whatever a security enforcement officer sees, hears or learns of, which is of a confidential nature, will be kept secret unless the performance of duty or legal provision requires otherwise. Members of the public have a right to security and privacy, and information obtained about them must not be improperly divulged.

INTEGRITY

A security enforcement officer will not engage in acts of corruption or bribery, nor will an officer condone such acts by other law enforcement officers. The public demands that the integrity of law enforcement officers be above reproach. Law enforcement officers must therefore avoid any conduct that might compromise integrity and thus undercut the public confidence in a law enforcement agency. Officers will refuse to accept any gifts, presents, subscription, favours, gratuities or promises that could be interpreted as seeking to cause the officer to refrain from performing official responsibilities honestly and within the law. Law enforcement officers must not receive private or special advantage from their official status. Respect from the public cannot be bought; it can only be earned and cultivated.

COOPERATION WITH OTHER OFFICERS AND AGENCIES

Security enforcement officers will be responsible for their own standard of professional performance and will take every reasonable opportunity to enhance and improve their level of knowledge and competence. An officer or agency may be one among many organisations that may provide law enforcement services to a jurisdiction. It is imperative that a police officer assist colleagues fully and completely with respect and consideration at all times.

PERSONAL/PROFESSIONAL CAPABILITIES

Security enforcement officer will be responsible for their own standard of professional performance and will take every reasonable opportunity to enhance and improve their level of knowledge and competence. Through study and experience, a police officer can acquire the high level of knowledge and competence that is essential for the efficient and effective performance of duty. The acquisition of knowledge is a never-ending process of personal and professional development that should be pursued constantly.

PRIVATE LIFE

Security enforcement officers will behave in a manner that does not bring discredit to their agencies or themselves. A police officer's character and conduct while off duty must always be exemplary, thus maintaining a position of respect in the community in which he or she lives and serves. The officer's personal behaviour must be beyond reproach.

Ethical Problems in the Use of Authority include the use of authority to promote personal values and avoiding.

Ethical Problems in the Relationship Between Personal and Professional Interests

- Using professional status to promote personal interests (religious, philosophical, financial, etc.)
- Using institutional time and materials for personal gain unrelated to legitimate work activity
- Engaging in or promoting professional activities that are contrary to personal values
- Engaging in public or private personal activity that is contrary to professional values (use of drugs, driving under the influence of alcohol, etc.)

Ethical Problems in Personal and Professional Commitment to Clients

- Behaving unethically in personal relationships with clients
- Using relationships with clients/public for personal gain (to acquire goods more cheaply, have work done for personal benefit, accepting gifts, etc.)

Ethical Issues in Criminal Justice and Public Policy

- The "War on Drugs;"
- Government policies having implications for criminal justice professionals in issues such as youth confinement, fingerprinting of juveniles, and compulsory treatment such as mandatory participation in substance abuse programmes or anger management;
- Capital punishment;
- The move away from rehabilitative juvenile justice policies toward more punitive policies;
- Policies involving harsher penalties resulting in "prisoner warehousing;"
- Government-imposed mandatory sentencing (three-strikes legislation, mandatory minimum sentences);
- Truth in sentencing policies;
- Increased surveillance of citizens in society.

Ethical Issues Resulting from Security Enforcement Policies

- Policing policy in domestic violence cases
- Police profiling
- Use of force
- Use of law enforcement agencies discretion

Ethical Problems in Information Sharing

- The ethics of withholding information; for example, from a client, the court, or the law enforcement;
- Problems of confidentiality and privileged communication; for example, counsellor/client relationships and participation in research;
- Rules or practices relating to the retention or disposal of court records; for example, in the juvenile system where some states are now considering making juvenile records and court hearings open to the public and the media.

Ethical Problems Dealing with Human Rights Issues in the Criminal Justice System

- The administration of cruel and unusual punishment;
- Human rights violations against prisoners (women, men, juveniles);
- Capital punishment.

Ethical Issues in the Media Reporting of Crime

- Crime and public opinion;
- Crime as entertainment;
- The politicization of crime.

There are many issues facing today's law enforcement officers and other law enforcement agencies. Some include the police use of excessive force, deadly force, law enforcement corruption, police pursuits and other popular police related topics. Irrespective of these, there are code of ethics guiding the profession. All police agencies throughout the country should be required to adopt the code of ethics as part of their policies and procedures. Each department should make it mandatory for officers to know as a

matter of training what the code of ethics document represents. The departments should hold annual ceremonies where officers renew their code of ethics and oath of office.

REFERENCES/FURTHER READING

Council of Europe (2002). The European Code of Police Ethics. Strasbourg: Council of Europe.

Haberfield, Maria and Lior Gideon (2008). Policing is Hard on Democracy, or Democracy is Hard on Policing? In Comparative Policing: The Struggle for Democratization, edited by Haberfield M. R. and Ibrahim Cerrah. Thousand Oaks: Sage Publications, Inc.

HCNM (2006). Recommendations on Policing in Multi-Ethnic Societies. The Hague: OSCE.

HCNM. Recommendations on Policing in Multi-Ethnic Societies." The Hague: OSCE, 2006. http://www.osce.org/hcnm/32227

Holmes, L. (2012). What are Police? In Toolkit on Police Integrity, edited by Pierre Aepli. Geneva: DCAF. http://www.dcaf.ch/Publications/Toolkit-on-Police-Integrity

Kolthoff, E. (2010). The Importance of Integrity in the Security Profession: Bringing in Human Rights. In Ethics and Security, edited by Monica den Boer & Emile Kolthoff. The Hague: Eleven Publishing.

Marx, Gary T. (2001). Police and Democracy. In Policing, Security, and Democracy: Theory and Practice, edited by M. Amir and S. Einstein. Office of International Criminal Justice.

Myhill, A. and Quinton, P. (2015). It's a Fair Cop? Police Legitimacy, Public Cooperation, and Crime Reduction: An Interpretative Evidence Commentary. London: College of Policing. http://whatworks.college.police.uk/Research/Pages/Published.aspx

OSCE (2008). Guidebook on Democratic Policing. Vienna: OSCE, pp. 9-17.

OSCE (2008). Guidebook on Democratic Policing. Vienna: OSCE. http://www.osce.org/spmu/23804

Prenzler, T. (2009). Setting Standards. In Police Corruption: Preventing Misconduct and Maintaining Integrity. New York: CRC Press Taylor & Francis Group, pp. 27-30; 33.

Stone, C. E. and Heather, W. (2000). Democratic Policing: A Framework for Action. Policing and Society 10, pp. 11-45. http://www.vera.org/sites/default/files/resources/downloads/stone_ward.pdf

Sung, Hung-En. (2006). Police Effectiveness and Democracy: Shape and Direction of the Relationship. Policing: An international Journal of Police Strategies and Management 29, no. 2. pp. 347-367.

UNODC (2011). Handbook on Police Accountability, Oversight and Integrity. Vienna: United Nations, pp. 5-8.

UNODC (2011). Introduction to Handbook on Police Accountability, Oversight and Integrity. Vienna: United Nations. http://www.unodc.org/unodc/en/justice-and-prison-reform/tools.html

SECURITY PRACTICE: NEED FOR STANDARDIZATION AND PROFESSIONALISM

Barrister Adebayo Akinade dfisn &
Brigadier – General Charles Adisa Bossman fisn

ABSTRACT
Standard work procedures are the "how" of tasks description and practice of operations of a profession. Standard work procedures provide the minimum standard of best practice which is an amalgam of disciplines that is moving inexorably towards professionalization. The idea of security as a profession remains as difficult and elusory as a comprehensive definition of security that captures all of its modern facets and many actors. The view of elevating such a discipline as security to the status of a profession provokes polarized opinions. This paper reviews the literature, examining what elements identify a security professional and exploring the significant themes and issues relating to protection practice. To support these elements, security experts will be exhausted using a multidimensional scaling technique to assess what constitutes a suitable and validated body of knowledge. It is concluded that many of the issues pivotal for progressing security towards professionalism are being addressed. However, there exists a need for research into developing a consensus and functional unity among the various branches of the security profession, and to identify emergent issues that affect security as a profession. One approach put forward by this paper is that a singular body of knowledge, in part, that can aid in the understanding of security.

1.00 INTRODUCTION

Security, as a concept, has diverse dimensions. It is aptly used in law, psychology, finance, information access, public safety, defense and military matters. Security is an important concept that every human person desires and it has one or two meanings though it defies precise definition. This account for the position of Barry Buzan (1991) who describes security as an ambiguous and multidimensional concept in which military factors have attracted misappropriate attention.

Security has to do with the process connected with assuaging any kind of threat to people and their precious values. This is why Buzan asserts that security is about freedom from threat and ability of states to maintain independent identity and their functional integrity against forces of change, which they see as hostile while its bottom line is survival (Bodunde, et.al, 2014). From the foregoing, security is generally agreed to be about feeling of being safe from harm, fear, anxiety, oppression, danger, poverty, defence, protection and preservation of core values and threat to those values.

William (2008) equally submits that security is most commonly associated with the alleviation of threats to cherish values, especially those threats which threaten the survival of a particular reference object. In line with the above, Imobighe states that:

Security has to do with freedom from danger or threats to a nation's ability to protect and develop itself promote its cherished values and legitimate interest and enhance the well-being of its people. Thus, internal security could be seen as the freedom from or the absence of those tendencies, which could undermine internal cohesion, and the corporate existence of a country and its ability to maintain its vital institutions for the promotion of its core values and socio-political and economic objectives, as well as meet the legitimate aspirations of the people (Ogaba. 2010:35-36).

The contemporary ideas and opinion about security are all-encompassing as rightly observes by Sola Ogunsanwo:

Security is more than military security or security from external attacks. For many inhabitants in the developing countries, security is conceived as the basic level of the struggle for survival. Therefore, in order to provide an integrated African Security Assessment, the non - military dimension of security should be added. Henceforth, security as a concept should be applied in its broader sense to include economic security, social security, environmental security, food security, equality of life security and technological security (Ochoche, 1997:27).

The role of security in society has evolved to encompass a myriad of disciplines, giving rise to challenges in defining a modern concept of security. This has been characterized by something of a cottage industry (Baldwin, 1997) that churns out definitional variations of security in a vain attempt to explicate the concept before it broadened further by political and social changes. The definitional difficulties that have plagued the concept of security have also extended to the roles of its practitioners. The problems of defining a profession appear to be at least as contentious as those of defining security, with reactions to definitions either polarized toward an unenthusiastic and uncritical acceptance or toward a rancorous and defensive rejection (Cogan, 1955). The combination of these two definitional conundrums naturally leads to some difficulty in identifying who or what constitutes a security professional. Despite these challenges, the evolution of the practice of security has been remarkably contemporaneous with the shift towards globalization.

Kavalski (2009), asserts that security is alone among professions which practice appears to be uncertainty, cognitive challenges, complex risks, and exasperation prompted by the heterogeneity of global life. It is the increasing complexity of the relatively young profession of security, which continues to keep step with an increasingly complex and interdependent world (Borodzicz & Gibson, 2006). The complexity results in the security professional being extremely difficult to identify and describe" the profession as multidimensional in nature, with many practicing domains and heterogeneous occupations (D. J Brooks, 2010).

There is no doubt that security at the macro-level qualified as a profession. This is pronounced in the components of national and multi-track security agencies such as Army, Navy, Air Force, the Police force, Customs, immigration, Nigeria security and Civil Defence Corps.

In each of the above remunerated security agencies, contain skills are required to accomplish the assigned roles. Those skills are acquired through vigorous training. In addition to the rigorous training programmed, members of each organisation are required to observe certain laid down ethics. In order to ensure strict compliance with the ethics of the profession, a body is put in place to regulate the activities of the organisation.

However, at the micro-level of security practice with individuals, the family, the organisations is related to private security practice.

Despite the fact that the private Guards Company Act, 1986, regulates the operations of private guards, it is still common to find quacks being employed as private guards. The promulgation of Nigeria Security and Civil Act of 2003 amended 2007 aims to ensure that private security practice is well organised to private professional services. Although, certain amount of skill and training are required of private guards, it is rather unfortunate that employers of private guards hardly attach much importance to the professional qualities expected of a guard. The implication of this negligence on the part of employers of private guards is obvious inefficiency with monumental consequences (Abolurin A. 2010). There is the need to move towards appreciable level of professionalism.
The following activities need to be considered for professionalism:

(a) Stipulating a minimum entry qualification for practice of security at various levels nationwide.

(b) Registration of private security practitioners at various tires of the private security system. Unregistered and untrained persons must not be allowed to practice at all.
(c) The Nigeria Security and Civil Defence Corps in collaboration with appropriate professional body should establish a distinct fees or salary structure for the private practitioners in the private and public sectors.
(d) Proper definition of progression grades for members, stipulation of entry level, which will graduate into highest level with regulated re-training and professional development modules.
(e) The curriculum of security education should undergo a thorough review so as to make it relevant to the needs of a modern growing multicultural and pluralistic society as ours.
(f) Designing an integrated ethical code of conducts, a legal bond formed by personal and corporate values.

There is the need for harmonized and standard code of ethics, credentials including education and training experience and membership in a professional society association or Institute.

This thrust towards professionalism is observable in the proliferation of active private security professional organisations and associations. There have been a lot of effects to produce professional security literature, magazines and books. Also, professional Institutes, colleges and Universities have developed security, protection service and safe courses at various levels of studies - certificates, diplomas, and degrees. (Akinade, 2016).

Despite numerous efforts to professionalize the field of private security, there are still many who feel that major obstacles need to be overcome. The most persistent one has to do with the education of the security guards, operatives and managers.

Proprietary guards, those hired directly by a company are generally better trained, and paid than their contract counterparts many guards, no matter whether they are contract or propriety are underpaid, undertrained, under supervised and unregulated. Minimal standards do exist in some places, but there is still a reluctance to train, educate and adequately compensate the guard force. Business considerations in making a product for profit can make it difficult for companies to see the need for paying so costly on security programmes. Thus, they often opt for the lowest - priced solutions no matter whether it affords real protection. Fortunately, this kind of thinking is undergoing a change as industry realizes its negative effects. This realisation will turn add pressure to industry to upgrade the position of security guards. Current Standards, code of ethics and educational courses need to be supported by industry participation.

Security increasingly includes protection against contingencies that might prevent normal company operation from continuing and from making a profit. The concept of risk management is further integrated into a comprehensive loss - prevention programme, the security function focuses less and less on enforcement and more on anticipating and preventing loss through proactive programming. Such challenges undisputedly require high - level security management and an increasingly well - increasingly group of security professionals.

2.00 AIMS AND OBJECTIVES OF THE PAPER

The purpose of this paper is to determine what elements identify a security professional through a review of the literature, to explore the significant themes and issues, and to identify any emerging issues. Therefore, the paper will consider a number of discrete objectives, namely:

1. What is the significance and relevance of training and education to professionalism in security practice?
2. Why is it necessary to be security professional?
3. What factors define and support the security professional?

4. What elements will most assist the drive to a security professional?
5. What are the features of a security professionals?
6. What are the codes of conducts and practice of security practitioners?
7. What are the prospects of professional security practice in Nigeria?

There is an ever-increasing reliance by both public and private sectors to deliver security, as public policing no longer has a monopoly on such services (Bradley & Sedgwick, 2009). It is important to be able to provide an understanding and demarcation of security discipline.

3.00 THEORETICAL FRAMEWORK AND CONCEPTUALISATIONS OF SECURITY

Securus is the Latin root of the English word 'security', meaning "free from danger" ***(Craighead, 2003),*** which according to ***Fischer and Green (2004)*** implies a stable, relatively predictable environment… without disruption or harm and without fear of disturbance or injury. In an observation, ***Borodzicz and Gibson (2006)*** point out that security should not be so much defined as an objective, but rather as a dynamic process that is responsive to time and place. The concept of security has gradually altered throughout history as a response to, and a reflection of, a changing society ***(Fischer & Green, 2004).***

Changes in social structure and perceptions may be gradual, or they may undergo sudden and dramatic shifts caused by events such as the terrorist attacks on New York and Washington in 2001. The advent of globalization and the information age has created the ability to broadcast news as fast as it occurs via "hyper coverage" ***(Reid, 2002),*** creating a "CNN effect" ***(Taylor, 2002)*** which compounds dramatic shifts in social perceptions, creating more pronounced, widespread, and swift changes in concepts such as security than at any other time in history. The world has undergone a dramatic shift in the perception of security in the last decade, creating the most significant changes to the field since the Second World War ***(Fischer & Green, 2004).***

Compounding the problem of identifying who or what constitutes a security professional is the difficulty in pinning down what constitutes a professional. ***Cogan (1955)***, attempts to clarify the term profession by identifying three levels of definition, including a historical definition, a persuasive definition, and an operational definition, ***(Cogan, 1955)***. A survey of the body of literature that attempts to define the term profession by the Interim Security Professionals' Taskforce (2008), revealed several key principles that embody the concept of profession across such occupations as legal practice, medicine, education and pharmacy, including knowledge, competency, learning, ethics, and membership within an association of peers (The Interim Security Professionals' Taskforce, 2008). More recent work by this industry driven group, part funded by the Australian Attorney-General's Department, includes attempting to raise the professionalism of the security industry by having a security practitioners register, based on the principles of professionalism (Australasian Council of Security Professionals, n.d.).

Traditional professions such as law and medicine meet each of ***Cogan's (1955)*** three levels of definition; however, the relatively young profession of security appears to suffer from somewhat of an image problem. In the past, the Interim Security Professionals' Taskforce (2008a) have cited a lack of understanding… of the difference between… those providing front-line operational services… and those providing professional services one of the key factors in limiting the contribution of security professionals to Australia's security and safety.

Borodzicz and Gibson (2006) present a useful framework, which identifies the four key internal drivers of security, as criminology, risk, terrorism and management. The shift in the conception of security in the 21st century has pushed security to the forefront of the criminological agenda ***(Zender, 2009).*** When security is considered as a criminological function, it naturally opens up the debate of public versus private security. According to

Borodzicz and Gibson (2006), security is no longer an exclusive organ of the State; it is now a commercial service industry available to those who can afford it. ***Crawford (2006)*** argues that perceiving security to be solely a function of criminology and policing tends to focus attention on "the question of who employs officers rather than the interests (public or private) that they serve. Security provides freedom from danger (Craighead, 2003, and freedom from danger naturally implies some level of safety. Safety is a value held by individuals, states, and other social actors… [and] may include physical safety ***(Baldwin, 1997). Kavalski (2009),*** states that the concept of security includes the need to seek safety and avoid harm. It is here that a criminological interpretation of security is insufficient, as security must encompass a wider range of risks "than simply those caused by criminal activity ***(Borodzicz & Gibson, 2006).*** Whether a risk is characterized by purely natural events or by human activity, either deliberate or unintentional, "it is likely that the security function will be involved in dealing with the consequences, particularly if unpredicted" ***(Borodzicz & Gibson, 2006).***

The pre-emption of risk, therefore, becomes the domain of security through risk management ***(De Goede, 2008).*** According to Standards Australia's Security risk management handbook, the management of security risk is a key and fundamental part of… wider risk management activities… [and] should be interlinked… with all other risk management activities ***(Standards Australia, 2006).*** The only difference between security risk management and the wider risk management activity is "the application of discipline specific knowledge ***(Standards Australia, 2006),*** suggesting that security holds a large enough body of knowledge to warrant a specific application of risk management. However, the distinction between security related catastrophic risks and those of a non-security nature is becoming increasingly blurred, expanding the security professional's portfolio to also include business continuity and crisis management ***(Omand, 2004).*** Paradoxically, it has largely been the response to the perceived increase in the risk of transnational terrorism that has stimulated the growth of security responsibility to encompass other crises.

As terrorism has lost its borders, so too has security in its role as a counterterrorism function. ***Lefebvre (2003)*** states that the transnational nature of several terrorist organizations… implies that their detection, disruption, and elimination can succeed fully only if done globally. As a result, there have been calls for further research into and development of transnational security networks ***(Wood & Dupont, 2006)*** as the increasingly transnational nature of security threats makes isolation an impossible option ***(Lefebvre, 2003)***. This has stimulated dramatic growth in private security, with transnational corporations… becoming increasingly important contractors of private security services ***(Abrahamsen & Williams, 2008)***. Nowhere has this been more infamously apparent than in Iraq where the United States military has increasingly outsourced many securities related activities, resulting in the blurring of distinctions "between private security companies, private military companies, and defence contractors ***(Borodzicz & Gibson, 2006)***. Now that it has gained momentum, the privatization of military activities has expanded to become global big business, raising fundamental analytical, political, and ethical questions ***(Abrahamsen & Williams, 2008)***

4.00 CONCEPTUAL AND THEORETICAL CLARIFICATION: PROFESSIONALISATION OF SECURITY

A review of the literature shows that security is continuing to evolve through the uncertainties of globalization and the information age ***(Kavalski, 2009)*** towards a "new professionalism" ***(Fischer & Green, 2004). Brooks (2006)*** is confident that security is moving towards becoming a more united discipline, as it becomes more professional, concepts are developed and defined, and tertiary education increases to support the discipline. At present, security appears to have begun its journey down the road to becoming a profession, and the question is now how far has it come and how

far does it need to go? In 2008, the Interim Security Professionals' Taskforce published a discussion paper (2008) with the aim of generating debate on a range of key issues facing security professionals including defining the security professional, key standards, professional status, education requirements, professional regulation and accountability, and professional unity. These key issues stem from five criteria identified as being the required characteristics for the security profession to be considered a profession in its own right. These include agreed and enforced standards of behaviour/ethics, standards of education, formal requirement for professional development, a college of peers and a distinct body of knowledge ***(The Interim Security Professionals' Taskforce, 2008)***.

Professionalization of Private Security Practice

By definition, a profession is an ideal type of occupational institution with a limited number of occupations or vocations involving special learning which carries so much social prestige. Functionally, ***Bennis (1969)*** defines it as a calling based on a foundation of knowledge towards a clientele and members of the profession". This is in agreement with **Carr-Saunders' (1996)** definition, which motes that a profession is "an occupation based upon specialised intellectual study and training, the purpose of which is to supply skilled service or advice to others for a definite fee or salary.

Professionalism simply refers to the ethos or expected standard of behaviours and performance of the professionals. It includes: the character, spirit and to distinguish a professional from an amateur.

The fact is that a professional status confers on the practitioner's notable benefits such as better public perception of the status of that profession to be higher that of just a job. There is the need to note that occupational prestige accorded to a specified stratum within specific occupation by the general public.

Another benefit of professionalization to a job-holder is improved deriving from the profession higher degree of bargaining furthermore, professionals control entry into the profession, limit entry as a form of social control which in apparent scarcity and the attendant prestige. This bestows on them, the power to apply the law of demand and supply.

(a) Professional Structural Attributes

For a job or occupation to be accorded a professional status, the following factor must be put into consideration:

i. It must be a full-time occupation. The practitioners should strictly devote and commit himself to the job as a life-lovely career.
ii. There must be established and duly accredited Institutions for the training of the members of the profession.
iii. Every profession must have a professional association of member who must be dignifying following special type of qualifications and licence to practice the profession.
iv. Members must put in place a regulatory code of ethics, and these are invariably enforced by the professional associations.
v. The professional body nurtures a clientele who has no choice but to accede to the professional judgement. In other words, clients are controlled by the professions approved stipulations with logical towards the practice and principles. ***(Akinade, 2016)***

(b) The Professional Attitudinal Features

The attitudinal attributes of a profession comprise the following:

i. **Expertise:** the Practice of a profession is rooted in a foundation of knowledge organised into an internally consistent function in the relevant body of knowledge.

ii. **Display of Authority:** The authority is derived from the professional expertise. This is variously known as "authority of competence, authority of knowledge". It is this unique authority that highlights the layman's comparative ignorance.

iii. **Self-Regulation:** Essentially, the professional does not subscribe to

snoopy bossing given the fact that he/she is a knowledgeable expert. He/she accepts collegial control. Basically, a professional must have the ability to make decisions without external pressure. His/her recourse is to the professional association as a major reference.

(c) Process of Professionalization

Professionalization is a process towards professionalism. It is a progression from the periphery towards the idea type of occupation. The process of professionalization involves the following:

i. Development of specialised skills and training such that the language of the profession sounds esoteric to the "uninitiated"
ii. Establishment of regulations, rules governing the profession
    a. Code of Conduct
    b. Fees etc.
iii. Formation of professional associations who laws define labour relationships career or occupational lives, individual and group-worth opinions and deep mastery of operating sentiments.
iv. Setting up a code of ethics for the members, emphasising such conduct as standard of work, dedication responsibility and emotional neutrality.
v. Stipulate minimum qualifications for entrance into professional practice and activities.
vi. Enforcement of appropriate rules and norms, sanctions of conduct among member.
vii. A conscious and planned attempt to raise the status of the professional group in the large society aside the workplace prestige.

5.00 EDUCATION AND TRAINING

Burnham (1998) states that professions emerged historically through a process of passing on an inherited body of knowledge that practitioners followed and professed. Professional bodies of knowledge are both academic and practical (The Interim Security Professionals' Taskforce, 2008) and therefore require both training and education in order to be passed on ***(Borodzicz & Gibson, 2006)***. How well defined is security's knowledge base has also been the subject of debate. It has been argued that security lacks a defined knowledge structure ***(Smith, 2001)***, and that much of the knowledge structure remains in the realm of expert knowledge ***(Abrahamsen & Williams, 2008; Smith, 2001***) making the task of providing appropriate education and training a difficult one ***(Brooks, 2006)***. In order to rectify this situation, the Security Professionals' Taskforce have proposed creating a security umbrella entity which would be tasked with, among other things, defining and promoting the development of formal bodies of knowledge and recognising the need for qualifications and competency standards ***(Security Professionals' Taskforce, 2008)***.

Strategic Plans and Structure for Actualization of Standardization of Professional Private Security Practice

The present arrangement should be reviewed and restructured so as to accommodate professionalism in the private security practice. The Nigeria security Civil Defence Corps, as a government body in collaboration with a professional body to be charged with the general duty of:

(a) Determining the standards of knowledge and skills to be seeking to become registered members of the private security profession and reviewing those from time to time as circumstances may require;
(b) Securing the establishment and maintenance of registers of persons entitled to practice as members of the profession and the publication from time to time of lists of those persons;
(c) Reviewing and preparing from time to time, a statement as to the code of conduct which the professional body considers desirable for the private security profession; and
(d) Regulating and controlling the practice of the private security profession in all its aspects and ramifications.

1. Composition of Board for Private Security Profession: A body should be established to manage affairs of the private security practice under Nigeria Security and Civil Defence Corps, since it is the statutory body establish to manage the affairs of private security practice.

The Board shall consist of the following members who shall be citizens of Nigeria

(a) The chairman, who shall be a security professional of not less than fifteen years post-experience to be appointed by the president, commander in chief of the Armed Forces on the recommendation of the Minister
(b) A representative of the Federal Ministry of Interior, who shall be the Commander-General of the Security and Civil Defence Corp
(c) The president of the Association of Licensed Private Security Practitioners
(d) A representative of Nigeria Police Force
(e) A representative of Nigeria Immigration Service
(f) Four (4) Director-General of security Professional Institutes
(g) One representative of the Armed Forces
(h) One representative Neighbourhood Watch (i) A representative of Fire Service.

2. The Register of Private Professionals

The **NSCDC** shall appoint a Registrar who shall perform the following functions:

(a) The Registrar shall be the secretary to the board of private security affairs and to the Disciplinary Tribunal (b) It shall be the duty of the registrar to prepare and maintain:

i) A register of the names addresses, approved qualifications and of all persons who are entitled to enroll as members of the private security professions;
ii) A register of the premises where members of the profession engage in their practices;
iii) To remove from the register the name of any registered person who has died or the persons whose temporary registration has ceased on directories of the council;
iv) To record the names of registered persons who are in default for more than six months of renewal of practicing licence.
v) To monitor the activities of register private security companies;
vi) Proper screening of the Directors of private companies and certify them to be fit and proper persons to operate private security companies;
vii) To issue licence to the qualified companies; and
viii) To be in charge of mandatory training and retraining of the employers and employees of private security companies.

3. Professional Discipline

It is recommended that a disciplinary tribunal is established which shall be charged with the duty of considering and determining any case referred to it by the investigating panel established by the council.

This body shall have a committee which shall conduct a preliminary investigation into any case where it is alleged that a person registered has misbehaved in his capacity as private security professional or should for any other reason be the subject of proceedings before the tribunal.

A person registered as private security professional is judged by the tribunal to be guilty of infamous conduct in any professional respect.

Rules and Procedures for the Practice of Private Security Profession

The statute has placed the following responsibilities on NSCDC:

a) For the training of suitable security practice methods, practice and strategies.
b) For the supervision and regulation of the engagement and training of persons or company practicing as private security practice.
c) Prescribing the form of license to practice to be issued annually or it thinks fit by endorsement of an existing

professional in default of renewal of practicing license.

d) Restricting the right to practice a Nigerian private security professional if the qualification granted outside Nigeria does not entitle the holder to practice as a security professional.

Registration as Private Security Professional

A person shall not be allowed to practice as private security professional in Nigeria unless he is registered by the Nigeria Security and Civil Defence Corps. A registered private security professional shall be entitled to practice throughout Nigeria if he is a Nigerian citizen and he is of good character and fit and proper person.

Such a person must have attended a course of training approved by the Nigeria Security Civil Defence Corps or the course conducted at an institution approved by Nigeria Security Civil Defence Corps.

He must have undergone the statutory continuous professional training conducted by Institution recognised by the NSCDC or the Nigeria Security Defence Corps and has obtained a certificate of experience.

6.00 A CODE OF ETHICS AND CONDUCT

Ethical considerations are also one of the core issues at the heart of the debate over security professionalization. There are emerging issues that are receiving little research consideration, including the influence of globalization on emergent hybrid and transnational security practices ***(van Buuren, 2009). Evetts (2006)*** identifies standards and codes of ethics that are monitored and operationalized by professional institutes and associations as one of the key features of occupational professionalism. One of the broadly supported outcomes of the 2008 Security Professionals Congress was the development of an in principle statement for the advancement of security professionals, which states that associations involved with security professionals should have an enforceable code of ethics that recognizes the importance of stakeholders including the community, clients and professionals ***(Security Professionals' Taskforce, 2008***. Codes of ethics must be legitimized through some form of peak regulation, as well as through legislation and regulation ***(Borodzicz & Gibson, 2006). Pepper (2003)*** also argues that a code of ethics implies that there must be a governing body that will control the actions of members of the profession, and that security has no such governing body. The Interim Security Professionals' ***Taskforce (2008)***, proposed a variety of solutions to this issue, including an association of associations, appointing a lead association, or creating an associated society for all of the security related professional and industry associations in Australia. The Interim Security Professionals' Taskforce (2008) noted that even using the behavioural standards adopted by well-established professions, the question of a code of ethics for the security professional is a matter for considerable discussion and debate.

7.00 PROFESSIONAL DEVELOPMENT

The concept of continuing professional development as a hallmark of professionalism is becoming more widely used in a variety of occupations workplaces ***(Evetts, 2006).*** Requirements for competency and continuing professional development are also one of the key elements of professional codes of ethics (The Interim Security Professionals Taskforce, 2008b). The Interim Security Professionals Taskforce (2008), identified four possible frameworks on which to base the standards, qualifications and continuing professional development requirements… for security professionals, including the Australian Qualifications Framework (AQF) which would be based solely on qualifications rather than a combination of qualifications and experience; certification levels based on responsibility and competence which would combine the AQF and relevant experience into a points-based system; a role-based requirements framework, where the level of experience in strategic, operational, and tactical responsibilities are used; or alignment with Security Risk Management Body of Knowledge (SRMBOK) Practice Areas and Activity Areas where the activities of security professionals are assessed against five practice areas (The

Interim Security Professionals' Taskforce, 2008). The disciplinary diversity of modern security also creates challenges in the area of professional development, and developing functional unity among the various branches of the security profession is another issue requiring further research.

A College of Peers

A college of peers refers to an association or organisation of people with a common interest, religion, or profession (The Stanford Digital Forma Urbis Romae Project, n.d.). According to the Interim Security Professionals Taskforce— renamed Australasian Council of Security Professionals (n.d.; 2008a)—a college of peers would provide security professionals with arrangements that link peers together and recognise other practitioners of the discipline as their fellows (p. 28). Hadorn et al (2007) state that any attempt to integrate transdisciplinary research requires the development of integrative methodology and a college of peers. Given the transdisciplinary nature of the security profession, and the need for some form of functional transdisciplinary unity, a college of peers provide a focal point peer association and the establishment of ethics and standards (The Interim Security Professionals' Taskforce, 2008).

A Body of Knowledge

There is some debate as to whether there exists an adequate body of knowledge to meet the needs of the criteria for professionalization of security (Pepper, 2003). Morin (cited in Knyazeva, 2004) laments over the disjointed, piecemeal, compartmentalized state of human knowledge in general, although his discourse is remarkably applicable to the state of security's body of knowledge, which is also increasingly poly-disciplinary, transversal, multidimensional, transnational, [and] global. This view is echoed in Bergin, Azarias, and Williams (2008) argument that security practitioners' lack of mutual understanding and respect for each other's knowledge is a key factor that has limited the successful interaction between [security] sectors. Cogan (1955) asserts that a profession requires a unified body of knowledge, which cannot be achieved while there is a dearth of adequate standards that define the knowledge expected of the security professional (The Interim Security Professionals' Taskforce, 2008). However, there have been a number of studies that have put forward relevant security bodies of knowledge.

8.00 FOSTERING AND MENTORING IN SECURITY PROFESSIONAL PRACTICE

Training and retraining coupled with carefully planned mentoring scheme play crucial role in sustaining professional growth and development in security practice and organizations

Mentoring occurs usually when an experienced member of the profession assists others to grow and understand the rudiment of the security practice. Indeed, several well-organised profession models rely on the tradition of training and transferring skills to younger members of the profession.

Besides, under a mentoring arrangement, both partners benefit, indicating that the best way to learn is to assist in the development and teaching of others in the skills of practice of profession.

Mentoring takes place in all well-organized professional practice whether it is adopted as a policy or not. According to experts, modern day mentoring scheme entails absorbing the culture and perceived values of the profession through interactions with members. According to experts, the following factors are some of the reasons established professions adopt mentoring as training programmes:

- Inductions to help new recruits, trainees or graduates settle into the organization,
- Skills enhancement, to enable skills to pass on in the workplace by experienced, highly competent staff to others who need to acquire specified skills'
- Career development, to help staff in the planning, development and management of their careers and to help them become more resilient in times of change, more self-reliant in their careers and self-directed learners.

- Affirmative action, to assist aggrieved subordinate staff to redress the imbalance at higher levels in organizations, provide support and help overcome barriers that often block their progress,
- Leadership and management development, to encourage the development of competences more easily gained through example, guided practice or experience than by education and training,
- Education supports, to bridge the gap between theory and practice. Formal education or training is complemented by the knowledge and the hands-on experience of a competence practitioner,
- Organizational development and culture change, to share the values, vision and mission of the
- organization. To communicate and work on a one-to-one basis to develop required changes, and
- Customer service, to model desired behaviours, encourage the development of competences, motivate for service quality, and above all to cultivate the right attitudes, among others.

Need for Mentorship in Professional Training for Enhanced Services and Performance

The function of professional training is to empower an individual with practical training that will enable him or her to competently provide security and safety services. Professional training is necessary because it enables the student-in-training to obtain a measure of experience of the issues involved in professional practice.

It aims to provide the required high standards that are necessary in the security and safety profession. After a security practitioner in training has acquired sufficient knowledge and experience in security and safety practice, he or she should be able to advance on the next step which is the application of gained knowledge and the attainment of further experience that his or her security and safety duties would bring forth, such as self-confidence and there be handling of professional issues independently.

Security practitioner in training should be mentored and nurtured by a highly experienced practitioner to gain a high standard of professional experience. The maintenance of high standard and quality performance is extensively important and vital for the future of the next generation security and safety practitioners.

Mentorship is highly important so that the practitioners' in-training can ascertain where their faults or mistakes and advance reside. Thus, any training must include a sort of assessment and interaction which will assist in structuring their disadvantages to advantages and their wrong faults to positive performance. Without this assessment the security trainee can be considered deficient.

This aspect of professional training method is highly advantageous to all security systems because it provides a sort of latency period for the new practitioners, where the trainee put into practice their professional experience. The pupilage aids in the maintenance of standards because through it newly security practitioners are able to perfect their acquired knowledge and skill before recruiting into real security practice.

Effective mentoring programme are goal-oriented and focus on the trainee's skill. Knowledge, and/or attitude development. It is very important that the trainee to have plan of development before they come into contact with a mentor. It is believed that people learn best by observing experts and by being given assignments. One of the main role and responsibility of the mentor is to review the progress of the trainee and to keep him accountable for what he does. Mentoring is a mutually beneficial arrangement because both the mentor and the trainee benefit from the exercise. As far as the trainee is concerned, he will be able to tap into the rich experience and teaching strategies of the mentor.

Enforcement of morals and professional ethics involve use of law to make effective standards

of good behaviour by all professional personnel of security and law enforcement. Heavy responsibility is placed on the shoulders of the leaders of security profession and law enforcement agencies.

Professional mentoring is an active social intervention associated with a wide range of beneficial outcomes for young people. Supportive relationships with non-parental adults can have a powerful and positive influence on the course of young people's lives.

9.00 PRACTICAL DEMONSTRATION IN THE SECURITY TRAINING PROGRAMME

Practical Demonstration Training Programme is for the maintenance of standards in security practice in Nigeria. There has been a major concern in the country's private security practice. The complaints in many quarters are of perceived fallen standards in security practice. There are many reasons for this steering from the societal values of trying to reach the top or rich quickly as possible.

As an integral part of training, there is the need to have in security training courses, practical professional exposure in the Public Security Agencies and Private Security firm. This programme will enable the student trainee understudy security processes, procedures, mannerisms and observation of the practice in action. This aspect of security education represents the point of contact between experienced practitioners and security trainees and protective actions.

The importance of practical professional exposure cannot therefore be underestimated. During the period of training, there should be extensive interaction and very lively sessions between experienced security practitioners which will be beneficial to all the parties concerned. It is suggested that since not all private security firms are fully equipped for security practical exposure programme, a refreshed list of security firms must be prepared for physical inspection of facilities and a project report on the practical experience be submitted. This programme must be undertaken by, all professional security trainees as a matter of compulsion and feedback should be in the firm of report as to the outcome of the programme.

This practical programme should be an accepted tradition or norm that every trained person to be a professional security practitioner should venture into the practice of security after understudying a professional practical demonstration programme in a recognized public security agencies or private security firm. This tradition will ensure the maintenance of standards in the profession. There should be a piece of legislation that would enforce professional. practical experience in the security profession.

The future of the security professionals particularly its survival is linked to the quality of security education and training received by the practitioners in their formative years, precisely in the University and professional institutes.

The complaints that standards of every facet of security practice is falling is real. The solution does not just lie in vowing to arrest the deteriorating situation. There must be an assessment of the scope of the damage to our security system before we can mete out remedial action. Anything short is illusory and will not serve the security profession well.

The Institute of Security Nigeria appreciates that there are shortcomings in the practice of security particularly in the private sector. What it does not know, especially is the scope and the magnitude of the problems and contributory factors to the falling standard.

There is therefore a compelling urgent need not only to return to the basics but to advance the frontiers of security education and training by embracing modern techniques. There is the need to evaluate the curriculum for the training and to confirm as to whether the current curriculum is in line with the global best practice. The substance of a robust and clearly articulated security education and training curricular is of paramount interest to the Nigerian public.

From time immemorial, the nature of threats to human life and well-being has continually changed and so have emerged strategies for dealing with them particularly in security field. The demands for improved security practice increased with advances in knowledge, research and new discoveries. The influence of philosophers and other great thinkers on an increasingly enlightened knowledge and skill, which facilitate innovations in the profession. There will always be the need and a place for security professionals highly skilled in the profession with a well-equipped and conducive environment for practice.

There is the need for repositioning and professionalizing the private security practice and appropriate regulation introduced into the practice for enhanced performance and productivity. It is vital for the government to introduce some professional changes which should include introduction of mandatory training requirement for all security guards, officers and managers to license before practice. The aim of this legislation is to increase the professional, knowledge and skilled - base of the individuals thereby increasing the level of safety enjoyed by both the practitioner and the public.

The professional positions of the future security practitioners should be determined. What are the prospects of practice in developing countries like Nigeria? Our current situation, especially in the developing world still seems grim, but not hopeless. Nonetheless, it is vital to draw attention to the following essential points for reflection:

(I) The private security industry should be made to be:

a) Attractive to skilled labour.

b) Make integrity the watchword of the industry in order to gain the trust of the public.

c) Ensure competence for enhance service delivery.

A system that is driven by the following virtues and qualities be initiated in the practice of security:

(a) **Attractiveness:** To make the private security guard industry more competitive in Nigeria so that it will attract ONLY professionals.

(b) **Integrity:** To evolve a systematic way of regulating the manpower of private security guard industry in order to earn the trust of clients and ensure integrity.

(c) **Competence:** To introduce a system of continuous training and retraining of private guards in order to ensure competence and professionalism.

(II) Modern professional security practice continues its Onward march world-wide. We must not lose our focus. Security professional must be acclaimed on their contribution to their new ideas in protection service, research, scientific and technological discussion not merely for their technical operative skills. Optimum security service must be maintained and carried on in future by the new generation of security professionals.

10.00 PROFESSIONAL SKILLS, EFFICIENCY AND EFFECTIVES ENHANCES PROFESSIONALISM

The paper appreciates the bodies of knowledge studies that focused on what could be considered appropriate security. These programmes included an introductory course in organisational security (Nalla, 2001), Integrated Framework of Organisational Security (Brooks, 2009), Security Risk Management Body of Knowledge (Talbot & Jakeman, 2008) and ASIS International Symposiums (ASIS International, 2009). The integration of these studies and multidimensional analysis resulted in a singular framework of security.

Security Bodies of Knowledge

Nalla (2001) explored the core components of an introductory course in organisational security, where nine security topics were ranked important drawn from benchmarking security textbooks, security professional's interviews and proceedings of the ASIS first academic/practitioner symposium. The study emphasized, to a lesser degree, the consensus

on the conceptual and methodological components of security education such as fire safety, workplace violence and workplace drug use. However, this study was considered too narrow in approach and lacking core and relevance put forward by others, such as Brooks (2008; 2009), ASIS International (2009), and Talbot and Jakeman (2008).

11.00 PROFESSIONALISM THROUGH A BODY OF KNOWLEDGE

Simonsen (1996) has argued that security may be considered a profession, due to the fact that individual groups of security practitioners are approaching fulfilment of a set of criteria consisting of standards and ethics, a body of knowledge, a recognised association, a certification program, and an educational discipline. Nevertheless, ***Pepper (2003)*** argues that security is not a profession due to its failure to meet certain criteria such as those normally expected of the medical and legal professions, such as a having a governing body to regulate standards and ethics, and it's relatively a small body of knowledge. However, holding security up the standard of the medical profession may be misleading. According to ***Burnham (1998),*** it was twentieth century historians that began treating medicine as the model profession based on a definition of profession that involved altruism and power, of which medicine, of all professions, had the most of both ***(Burnham, 1998).***

If a combination of philanthropy and authority is the necessary standard of professionalism to which all other professions must be measured, one wonders whether the legal profession could still be considered as such. ***Simonsen (1996)*** may see the glass as half full and Pepper (2003) may see it as half empty, but either way, there is something in the glass. Given the ambiguous arena ***(Brooks, 2006)*** in which security resides post-9/11, the difficulty in defining the security professional is knowing where the definitional boundary lie today and where it may lie tomorrow. Nevertheless, the article has put forward a body of knowledge developed from others that may allow some of issues raised in this article to be addressed and boundaries presented. Once such a consensual body of knowledge has been validated and supported at the tertiary level, some of the other professional elements such as education and training, professional development and a college of peers may have a better opportunity of being achieved.

Efficiency and Effectiveness Enhances Professional Security Best Practices

Definition of Efficiency

Efficiency refers to the relationship between the resource inputs consumed and the outputs of goods, and services produced. Efficiency, expressed as a percentage, compares performance in terms of output/input ratio to a standard ratio representing the expected level of efficient person one who utilizes all resources (human, material, equipment, buildings, etc.) property and fully to obtain an optimum yield. The terms efficiency and productivity are commonly understood to mean the same. However, in Industrial Engineering terminology, "productivity" is simply an output /input ratio. When it is compared to a standard ratio and calculated as a percentage it is known as efficiency. Efficiency and Related Concepts.

To understand efficiency, we cannot look at it in isolation. Instead, we must look at it in relation to other dimensions of performance such as economy, effectiveness, and the quality and level of service. The relationships are explained below:

1. Relationship to Effectiveness

Effectiveness indicates the extent to which a programme achieves its objectives, goals or other intended effects. Therefore, a programme and its activities and operation must be selected and planned with care so that they can produce the goods and services which will meet the programmes' objectives. Thus, effectiveness relates to results. In contrast, efficiency relates to process and production cost.

When we measure efficiency, we must whether all the outputs produced are necessary for a programme to meet its goals. Theoretically, it is possible for an organization to be highly efficient but ineffective because it

happens to be doing wrong thing conversely, an organization could be inefficient but effective because it is doing the right thing, but is going about it the wrong way.

If an organization is to be cost-effective, it is necessary for it to be efficient and effective. That is, the organization should be doing the right thing in the right way. Ideally, the public service managers must manage the government programmes economically, efficiently and effectively to achieve maximum value for tax money spend. However, in reality, managers may have to make trade-offs among the three "E's" as appropriate to achieve acceptable results.

2. Quality and Level of Service

The efficiency of an operation is influenced not only by how much goods and services are produced, but also by the quality and other characteristics of out puts and the level of service offered. When the quality of production increases, the quality of work may decline at some stage. If one is concerned more about quality, volume may suffer as a result.

Therefore, in measuring efficiency, we must look at the quality and level of service in addition to the quality of outputs to property interprets changes in efficiency. A manager should understand the interrelation between the volume of production and quality and level of service. This is necessary to make trade-off decisions, that is, to balance quantity of output against quality in order to provide a service which is acceptable in both respects.

Some hypothetical examples of standards of output quality and level of service are:

- Error level in cheques issues should be less than 1%.
- A minimum mail delivery of once per day.
- 90% of passports should be issued within 3 working days.
- A maximum acceptable customer complaint rate of 5%.

3. Measuring Efficiency

Efficiency is calculated by comparing performance in terms of output/input ratio to an acceptable standard ratio (representing the expected level of efficiency) and express as a percentage of the standard. To measure efficiency, we must measure both inputs and outputs. These measurement concepts are explained below:

i. Measuring Resource Inputs

Resource inputs can be measured in many ways. For example, labour resourced can be measured in terms of salaries. Inputs can also, be measured in terms of operating and maintenance costs including salary cost. Total cost including capital cost is another unit of measure that should be considered when a significant amount of capital is used in an operation. In all cases the measuring units chosen should be appropriate and should represent all significant resources consumed.
For example, an output/input ratio could be expressed in any one of the following manners:

- Number of passports issued per person-year.
- Number of minutes per passport or number of passports per hour.
- Production cost per passport (unit cost).

ii. Measuring Output

In order to be measuring, outputs must be separate from each other, and uniform in their characteristics. Output of repetitive production processes meet these criteria, and therefore we can measure them by using and work measurement techniques.

Special projects, research work, continuing administrative support work, policy development, advisory functions, management overhead, etc. do not normally produce putouts which meet the criteria stated above. Rather they are examples of work which is difficult to measure. Some crude measures like ratios of overhead cost or person-year to the total cost or person-years, and comparison of staffing patterns between similar organizations may provide a rough indication of the efficiency of such difficult to

measure work. This rough measure should be used with caution and the results obtained should be analyzed and interpreted properly.

iii. Standard of Efficiency

The out/put ratio by itself does not indicate whether the performance it reflects is satisfactory or not. We need a reference point or benchmark to asses' performance and to measure changes in efficiency. By using one of the established work measurement techniques, standard of efficiency can be set, against which performance can be measured.

Performance can be assessed reliably by comparing it to engineered standards. An engineered standard is a specified duration of time, determined by work measurement, required to produce one unit of output or service or to perform a task. Engineered standards represent the concept of a fair day's work expected from an average employee with reasonable training and work experience. Specialists trained and experienced in individual Engineering or Time and Motion Study techniques develop these standards.

It may be difficult to develop engineering standards for some complex and variable work. In these instances, present performance can be compared with performance during a typical base period in the past. Such a base period output/input ratio is known as a relative standard. This type of a standard has a weakness in that it assumes that the expected level of efficiency has been achieved in the base period selected. Therefore, a proper analysis of the representativeness of the base period is necessary to ensure that such a standard reflected an acceptable level of efficiency.

Use of Standards in Management Controls

Performance standards are used for different purposes in various information and control systems. For example, performance standards are used:

- To demonstrate achievement of results by comparing performance data to standards of goals
- To plan operations and budget resource requirements.
- To improve productivity because they provide data for comparing present and proposed method and procedures.
- To provide a rational basis for pricing goods and services for cost recovery purposes.
- In production control and quality control system.
- For making trade-off decisions between efficiency and level of service.
- To indicate to employees and supervisors what results are expected of them. Therefore, standards are useful in appraising the performance of employees and in motivating them.

Measurement and Improvement of Efficiency

Measuring efficiency to develop a plan for improving it and to prove that such a plan has in fact yielded results. By merely measuring efficiency, we do not necessary improves it, but an organization is likely to be efficiency-conscious when its efficiency is measured and made visible.

Some possible ways to improve efficiency are listed below:

- Analysis of alternative means to choose the most economical and efficient way to provide the goods and services necessary for the accomplishment of programme goals.
- Structuring the organization in an appropriate manner so that it can operate with a minimum of delay and duplication.
- Planning the operation with due regard to the economics of scale.
- Planning the operation with resources just sufficient to handle the forecast workload in order to make the most of these resources.
- Production planning and scheduling to minimize production delays, work backlogs, staff waiting and idle time, etc.
- Continuously reveling work methods and procedures to simplify them. Using labour -saving devices and capital

equipment to increase productivity and using operations research techniques to maximize efficiency of operations when complex decision variables are involved.
- Selecting suitable employees and training them on the job to work efficiently.
- Motivating the employee to do a fair day's work. The use of efficiency standards to set production targets for employees and to monitor their performance against these targets.

The first issue is, given the quantity of material written on effectiveness and programme evaluation, what does it means?

Definition of Programme Evaluation

There is no universally accepted definition of evaluation. Basically, it is an attempt to learn from experience, particularly about the best way to achieve an organization's objectives. There are three issues which are central here:

1. Programme evaluation determines both positive and negative impacts including both intended and unintended impacts of the programme.
2. Focuses on the past performance of programmes - this retrospective.
3. Should help the decision maker determine whether the programme should be continued as is, expanded, modified, reduced or eliminated.

The important point to bear in mind (and which will be addressed in the next section) is that programme evaluation is first and foremost a management tool. In this context, it fits appropriately, with both planning and the accountability of senior management. Planning should make explicit the programme logic, that is why this programme form has been chosen to meet these programme objectives. As such the necessary project control to keep the programme-oriented to these goals should be in place and monitored. Both of these will serve reduce the repetition of mistakes.

Accountability means that beforehand there should be an explicit identification of what the programme will be responsible for achieving. Finally, programme evaluation will measure and report on the extent to which objectives are in fact achieved. However, this can only be done of the condition in planning and accountability has been met. In order to ensure that senior management is aware of potential benefits and costs of evolution it is perhaps useful to identify the main question with which management should be concerned when a programme or effectiveness evaluation is to be undertaken.

The questions which should be asked include:

- What should be evaluated, that is, what are the specific programme elements or components in which management is interested and about which decision are be taken; When should the evaluation be done, that is, at what time would it be most appropriate to undertaken the evaluation and ensure information is available to management for future decision;
- Who should do it? Particularly important here is the extent to which outsiders or those who might be more objective about the programme should be put in charge of such an evaluation. This must be traded-off against the fact that programme management has in-depth knowledge and information which would be extremely useful in any evaluation. What procedures are needed to ensure reliability and reasonable cost? This is particularly important when outside organization until is used for the evaluation in order to ensure that costs and/or the scope of the evaluation do not exceed, or are less than, the anticipated and predetermined levels which are necessary.

Efficiency, Morality, and Codes of Ethics in Security Practice. One should not attempt to evaluate security agencies and law enforcement officers by a cursory glance at their buildings, uniforms, vehicles, press notices, nor should one attempt to evaluate a

law enforcement agency or officer merely because the community, to all outward appearances, seems to be infested with crime, or free from it.

Any objective and scientific measurement of security agency or law enforcement officer should involve four considerations: efficiency, morality, legality, and compassion.

(I) EFFICIENCY AND EFFECTIVENESS

The measurement of security officer is most difficult. One should not confuse efficiency with effectiveness. An agency may be highly efficient, but most ineffective in accomplishing the goals of law enforcement and security operation.

For one reason, units of work measurement that are standardized for the vocation are not yet available. How many criminal cases should a police station issue in a day or work? How many reports should be handled by the patrol unit each night or month? How many cleared cases should the robbery squad produce each month or year? How many prostitutes should be arrested each month? It all depends.

It depends upon community support and cooperation. It depends upon the quality of security administration and supervision. It depends upon the competence, quality and integrity of the individual security officer. It depends upon the quality of the local bench. It depends upon the effectiveness of the security agencies. It depends upon the effectiveness of the local security officers. It depends upon the general quality of municipal, country, state, and federal government units in the area.

Can we rely upon criminal statistics to determine if we are undermanned? If we have a satisfactory ratio of civilian employees? If we have crime rates proper to our jurisdiction and its environment? If we have a satisfactory clearance rate for major crime? If our arrests are sufficient? If the amount of property recovered is sufficient? If the trend of crime is abnormally high? No, we cannot rely upon criminal statistics to give us absolute determinations. Even though they have been collected for a relatively short period they have an age-old deficiency: they are but averages, telling us what may be, but not telling us what should be.

As we improve the selection process for law enforcement and get better personnel; as we improve our administrative and records processes; as we receive closer cooperation from the public; as we improve our methods of investigation - will we not have more arrest and successful prosecutions? Of course, and yet some will point to a crime wave, and as is so common, rise up in righteous indignation and demand a "get tough" policy and the need for "cracking head". Very few will think about the matter of statistical limitations, their veracity, and question every datum, frequency distribution, and interpretation.

It is believed that in accomplishing the police task with the least amount of money, manpower, facilities, and equipment, and at the same time, with the greatest success in achieving goals. But the fact is that most police agencies are to undermanned, underpaid, under trained, under supervised, under equipped, and under supported to be able to perform in a professionally efficiency manner. Enrico Ferm, the Italian criminologist, pointed out that society has the criminality it deserves. The authors would point out that most communities have the level of police service that they deserve.

The greatest improvement in police efficiency will come about, not by applications of computers to police deployment, not because a fleeter patrol vehicle has been engineered, and not due to new buildings. The greatest improvements in police efficiency will ensue when attention is forcefully directed to obtaining the very best of talent available from the nation's manpower pool, educating and training it to the limit of its capacity, and moving it up through the ranks as quickly as it is able to accept and discharge its responsibility. This talent will bring undreamed increases in efficiency - but with it, the greatest of headaches - for it will be merciless in eliminating archaic and Neanderthal attitudes and practices, demanding the utmost of dedication and

production of all members of the vocation, and mandating professional example in all aspects of the service.

This is not to depreciate those few planning and research units now operating in our larger cities - they are doing difficult task and service, and contributing substantially to agency improvement. But, the finest planning and research unit in the nation must still depend upon agency personnel for the implementation of its recommendation, and if that personnel is deficient, its work is largely in vain.

This is not to depreciate those highly motivated law enforcement professionals who are currently exemplifying the finest ideals of Nigerian law enforcement. This is to say that there is so great a need of them in the Nigerian law enforcement service today that we must make maximum efforts to recruit and enroll more and more men and women of the greatest capacity and character if we are impressive increases in efficiency.

Certainly, when we approach the area of efficiency, we can identify major police goals: the prevention of crime and disorder; the preservation of the peace; and the protection of life, property, and individual freedom.

And, certainly, we can identify major police methods: crime prevention; crime repression; regulation of non-criminal conduct; provision of service; and protection of individual freedom. And, certainly, we can identify the major line, staff, auxiliary, and special activities. Yet, a variety of opinion differs according to the level of Service – local, country, private, state, and federal; according to the region and according to the community. The fact is, there are no universally imposed or accepted standards for police administration and operations. For one reason, there does not exist nationalized police in our nation; for another, the philosophy of local autonomy precludes the imposition of a single pattern of policing.

Certainly, we can identify major criteria of goal accomplishment: the absence of crime, disorder, congestion, accidents, and conflicts within the community; adequate (at least at some comparable average) rates of arrest, clearances, property recovered, and successful prosecutions; minimum employee ratios and minimum per capital cost consistent with adequate (at least at some comparable average) performance; and, the absence of community complaints regarding police services and personnel. A variety of opinion lays that to such yardsticks, depending upon level of service, regional location, and community values.

Both the goals (with the implementing functions and activities) and the criteria or measuring rods for evaluating success are closely identified with the local environment, with the philosophy of the local police agency, with the force of community opinion, and with the value system of that particular region.

Certainly, we can identify major factors which relate to successful goal accomplishment: adequacy of administrative talent to plan, organize, direct, coordinate, control, and evaluate agency activities; adequacy of management talent to ensure the propriety, effectiveness, morality, and legality of agency policies, procedures; adequacy of fiscal process to ensure provision of necessary facilities, equipment, and manpower; adequacy of personnel processes to provide for the proper selection, training, regulation, and motivation of personnel; arid adequacy of public relations and human relations processes to provide for the development and maintenance of public cooperation and goodwill. The proper identification of such factors, must be done at the local level - not imposed from above - for such factors will vary with agency's goals, criteria for goal accomplishment, and with the unique characteristics of the agency and the community in question.

It is necessary to indicate that enthusiastic support for the movement to install planning and research units in law enforcement agencies. They must also indicate their strong belief that the finest planning and research unit will become frustrated and comatose if

the top-level leadership does not proceed to implement the obviously necessary recommendations, and to install audit and follow-up processes to guarantee complete implementation and continuing support for the recommendations.

There is a heavy responsibility placed on the shoulders of the police executives who install such a unit, for their studies may recommend, and adequately justify, changes which are radical and which may upset decades of unquestioned practices, and thus place the executive squarely upon the spot. If he makes an implementation of the recommendations, he upsets the equanimity of all personnel who are absolutely committed to the status quo; if he rejects, or table the recommendations, he may be tabbed as a bottleneck to progress. That is why it is most encouraging to note the development of such units in the police service, the implementation of their feasible and practicable recommendations, and their increased prestige - for the kind of development reflects great credit upon the law enforcement administrator and his commitment to the goal of ever-increasing efficiency.

(II) ENFORCEMENT OF MORAL

A group's "morals" or "morality", or "moral behaviour", or "moral positions", or "moral convictions are called an anthropological sense. All of these refer to whatever attitudes the group displays about the propriety of human conduct, qualities or goals. At times, we use them in a discriminatory sense. Here, we use them to offer limited but important sort of justification for an act, when the moral issues surrounding that act are unclear or in dispute. Put differently, morals, from `morality', are standards of behaviour, for example, in matters of sex. Morals also deal with the question of fair play and harmony between nations, classes and individuals. Morals, for example, exhort you to have your neighbour in contemplation as being directly affected when considering your acts or omissions which are called in question.

In religious parlance, morals involve doing to others as you would have them do to you. All these are summed up by Apostle Paul when he exhorted the Philippians to think on those things that are true, honest, just, pure, lovely, of good report, virtuous and praiseworthy.

Morality is therefore concerned with standards or principles of good behaviour. There is a general agreement, for example, the human beings ought to be honest, kind and helpful to one another. These are matters of morality. Private morality deals with those values which affect the individual concerned. Public morality deals with those values which affect the society as a whole.

Enforcement of morals could, therefore, be defined as the use of law to make effective some standards of good behaviour. This could be done either by imposing duties or by limiting liberties. Moral rules, according to C. S. Lewis, are directions for the running of the human machine. Every moral rule is there to prevent a breakdown, or strain, or a friction, in the running of the machine. That is why these at first seem to be constantly interfering with our natural inclination.

Some jurists believe that to speak of the enforcement of morals such is paradoxical. They contend that law and morals belong to two different categories of obligations. And if law and morals are two separates but overlapping systems each of which carries its own sanctions - and that is the model subscribed to both by Lord Devlin and by Professor Hart - then morals can only be enforced qua morals and law qua law.

There is no doubt that law has always enforced some morality. Even the most primitive legal order seeks to regulate matters such as homicide and theft. But the question is the limits within which law; in particular the criminal should be sued to enforce morality. The law should certainly intervene to prevent any unjustifiable immorally in persons or property. So, murder, rape, assault, arson, burglary, theft, etc.., are rightly treated as crimes as well as sins. Much the same may be said of demanding money by menaces 'for, however heinous the conduct of the person who is threatened may have, both morality and

law demand that this should not provide a weapon by which man may exploit another for his own purposes'.

But the real problem has been the argument that there is a sphere of private morality which is no business of the law; that what a man or woman does in private or what two or more sane, responsible adults may agree to do in private is exclusively their own.

Bentham and John Stuart Mill, for example, favour a rationalistic approach. Mill's emphasis is on the value of the maximum freedom for the individual which is compatible with the freedom of others. We shall discuss his theory in due course.

Evaluation of Morality

The Evaluation of Morality in practice of security is also most difficult:

Some people see the security practice as fundamentally a moral, as mercenaries who can and do make the transition from one regime to another without moral trauma. Some security officers regard obedience more highly than truth, beauty or goodness, and seeing obedience as the highest good, comes to believe that the police are the only truly moral force in society; hence moralistic (not necessary moral) police.

To become an increasingly moral person is to become an ever more mature personality. Maturity implies that capacity to surmount complexities with the realistic perception and decisiveness demanded by each unique situation. Morality is implicit in this process of making choices because our choices will be, in varying degrees, good or evil (and sometimes evil in their mediocrity).

Every choice, to some extent, is causative of a further humanizing or dehumanizing of self and/or others. To become more what we are meant to be (i.e. men) is good; whereas to act is such a way that we become fewer men is evil. To be moral is to be realistic: it is accepting the challenge of making what is to be, in fact. Men should be realists and treat men as men, relate God as God, and to the universe as what it is - in itself, and as man's basis, environment, and kingdom. In summary, we can say that the moral man lives and act psychologically according to what is true onto - logically (i.e. his gut-level decisions are consonant with the nature of being).

Thus, the moral man does not let things dominate him. To the extent that he does, he is not what man is meant to be: the ruler/developer of all other creatures. Neither does the moral man sell his mind or his soul (his principles) to another. To the extent that he does, he is a slave and not a man - for to be a man in essence, is to be free, to be capable of self-determination.

The proponents of moral believe in the most living thing for them to do is that which is most productive of dignity and honesty, and the goodness and humanness in the people involved in the decision. The spiritual concept of "love" is far from the saccharine, impulsive, and characteristic notion which our current era often reflects.

13.00 CONCLUSION

Members of the profession should be vision and leaders who work in an environment characterized by cooperation, collaboration, open communication and respect for all public safety and private security professional. Through training, technology career development and collaboration and integration with other public safety disc8plines, the overall quality and performance of private security professionals will become more responsive to security challenges in the nation.

This will increase the number of qualified, high caliber people who choose private security as a career and to increase the levels of professional employee retention indict-wide.

Bridging the knowledge and skill gaps through training in corporate, governance, capacity building, consultancy, standardization, advocacy and proffering on life, Fire and. Safety Security Risk management, is thus a strategic decision particularly important for compliance regulation, Business Continuity and Sustainable Development.

The key to success in security profession lies principally in EDUCATION AND TRAINING. The key opens the door to new knowledge, skill, new ideas, meaningful research, innovations, total commitment to the case of security and safety of people, teamwork, honesty, integrity and transparency. It empowers the people through a total commitment to their education and training and the eradication of ignorance. Selfless and visionary leadership would at least provide the much sought after behavioural role model, as well as the physical and infrastructural and human resources development (HRD) without which all other efforts fail. That key is certainly embodied in "TRAINING AND EDUCATION". As a matter of fact, the key opens the door to good professional performance, effectiveness, efficiency and productivity for the future generation of security practitioners.

The role of security in society has evolved to encompass a myriad of disciplines, giving rise to challenges in defining a modern concept of security. Compounding the problem of identifying who or what constitutes a security professional is the difficulty in pinning down what constitutes a professional. Security is many faceted and is a dynamic process that is responsive to time and place. Identifying a security professional by the practices and functions that currently define security is as problematic as satisfactorily defining security or profession in isolation. Security is continuing to evolve through the uncertainties of globalization, and so too is the burgeoning security profession. Although many of the issues that are pivotal in progressing security towards professionalism are being addressed, there exists a need for research into developing a consensus and functional unity among the various branches of the security profession, and to identify emergent issues that affect security as a profession, such as ethical considerations of transnational security practices. There is little agreement on definitions, but there is also little argument against the fact that the dramatic change in social structure and perceptions post-9/11 has changed security forever, and that change appears to be pushing security inexorably towards becoming a new profession.

REFERENCES

Abolurin, A. (2010), Security and its Management in Nigeria. I badan: John Archers Publishers

Abolurin, A. (2011), "Para-Military Agencies and the Promotion of Good Governance for National Security in Nigeria" in Ade Abolurin [ed] Nigeria's National Security: Issues and Challenges. Ibadan: John Archers Publishers.

Adedoyin, A. (2013), "An Appraisal of the Multidimensional Nature of Security in the Post-Cold War Africa" in African Journal of Stability and Development. Volume 7, No 2 Page 113-130.

Bodunde, D. 0., Ola, A. A. & Afolabi, M. B. (2014), "Internal Insecurity in Nigeria, The

Irony of Multiplicity of Security Outfits and Security Challenges" in IMPACT.- IJRHAL, Volume 2, Issue 5Page 213-220.

Buzan, B. (1991), "New Pattern of Global Security in Twenty-First Century" in

International Affairs [Royal Institute of International Affairs] pp. 431-451. Hubert, D. (1999), "Human Security: Safety for People in a Changing World" A Paper presented at a regional conference on The Management of African Security in the 21st Century, NIIA, Lagos 23-24June

Lippmann, W. (1944). U.S. Foreign Policy. London, Hamish Hamilton Maniruzzaman, T. (1982), "The Security of Small States in the World" in Canderra Papers on Strategy and Defence, No 25.

Ngbale, K. P. (2011), "Ethno-Religious Conflict: A Threat to Nigeria's National Security" in Ade Abolurin [ed] Nigeria's Notional Security: Issues and Challenges. Ibadan: John Archers Publishers.

Nwolise, 0. B. C. (2008), "National Security and Sustainable Democracy" in Emmanuel O. O. [ed], Challenges of Sustainable Democracy in Nigeria. Ibadan: John Archers Publisher.

Obasanjo, O. (1999), Grand Strategy for Notional Security. Abuja: Federal Ministry of Information, Page 1-3.

Ochoche, S. (1997), "Electoral violence and National Security in Nigeria" in African Peace Review. Vol. 1 No. 1 page 27.

Ogaba, 0. (2010), "Security, Globalization and Climate Change: A Conceptual Analysis" in Osita E. E. & Ogaba O. [ed] Climate Change and Human Security in Nigeria. Lagos: NIIA.

Orwa, D. (1984), "National Security; An African Perspective", in B. Arlinghaus [ed] African Security Issues: Sovereignty, Stability and Solidarity, Colorado: West View Press. United Nations Development Programme Report, 1994.

Walt, S. M. (1991), The Renaissance of Security Studies. Mershon International Studies Review, 41; 211-239.

Williams, P. D. (2008), Security Studies: An Introduction. London: Routledge Taylor and Francis Group

Abrahamsen, R., & Williams, M. C. (2008). Selling security: Assessing the impact of military privatization. Review of International Political Economy, 15(1), 131 - 146.

American Society for Industrial Security. (2002). Proceedings of the 2002 academic/practitioner symposium. The University of Cincinnati, Ohio: ASIS International.

ASIS International. (2009). Security body of knowledge (BoK): substantive considerations. Unpublished ASIS International Academic/Practitioner Symposium 2009, ASIS International.

Australasian Council of Security Professionals. (n.d.). The Australasian Council of Security Professionals. Retrieved August 20, 2010, from www.securityprofessionals.org.au

Baldwin, D. A. (1997). The concept of security. Review of International Studies, 23, 5-26

Bazzina, M. (2006). Security standards and support systems report: A collaborative project between the Commonwealth Attorney-General's Department and Standards Australia. Sydney: Standards Australia International Ltd.

Bergin, A., Azarias, J., & Williams, D. (2008). Advancing Australian homeland security: Leveraging the private sector: Australian Strategic Policy Instituteo. Document Number)

Borodzicz, E. P., & Gibson, S. D. (2006). Corporate Security Education: Towards Meeting the Challenge. Security Journal, 19(3), 180-195.

Bradley, T., & Sedgwick, C. (2009). Policing beyond the police: A "first cut" study of private security in New Zealand. Policing and Society, 19(4), 468-492.

Brooks, D. J. (2006). Mapping the consensual knowledge of security risk management experts. 7th Australian Information Warfare and Security Conference. Perth, Western Australia.

Brooks, D. J. (2008). Defining the science of security through knowledge categorization. Acta Criminologica, CRIMSA Conference Special Edition 2008, 1, 12-23.

Brooks, D. J. (2009). What is security: Definition through knowledge categorization. Security Journal, DOI 101057/sj.2008.18, 1-15.

Brooks, D. J. (2010, in review). Organisational security: Understanding practice boundaries from knowledge construct to a body of knowledge. Australian and New Zealand Journal of Criminology.

Burke, A. (2008). Fear of Security: Australia's invasion anxiety. Melbourne: Cambridge University Press.

Burnham, J. C. (1998). How the idea of profession changed the writing of medical history. Medical History Supplement, 18, 1-195.

Cogan, M. L. (1955). The Problem of Defining a Profession. The Annals of the American Academy of Political and Social Science, 297, 105-111.

Craighead, G. (2003). High rise security and fire life safety (2nd ed.). Woburn: Elsevier.

Crawford, A. (2006). Networked governance and the post-regulatory state?: Steering, rowing and anchoring the provision of policing and security. Theoretical Criminology, 10(4), 449-479.

De Goede, M. (2008). Beyond Risk: Premediation and the Post-9/11 Security Imagination. Security Dialogue, 39(2-3), 155-176.

Evetts, J. (2006). Short Note: The Sociology of Professional Groups: New Directions. Current sociology, 54(1), 133-143.

Fischer, R. J., & Green, G. (2004). Introduction to security (7th ed.). Oxford: Elsevier.

Hadorn, G. H., Hoffmann-Riem, H., Biber-Klemm, S., Grossenbacher-Mansuy, W., Joye, D., Pohl, C., et al. (2007). Handbook of Transdisciplinary Research. Amsterdam: Springer Netherlands.

Kavalski, E. (2009). Timescapes of Security: Clocks, Clouds, and the Complexity of Security Governance. World Futures: Journal of General Evolution, 65(7), 527 - 551.

Knyazeva, H. (2004). The complex nonlinear thinking: Edgar Morin's demand of a reform of thinking and the contribution of synergetics. World Futures: Journal of General Evolution, 60(5), 389 - 405.

Lefebvre, S. (2003). The Difficulties and Dilemmas of International Intelligence Cooperation. International Journal of Intelligence and CounterIntelligence, 16(4), 527 - 542.

Manunta, G. (1999). What is security? Security Journal, 12(3), 57-66.

Nalla, M. K. (2001). Designing an introductory survey course in private security. Journal of Criminal Justice Education, 12(1), 35-52.

Omand, D. (2004). Emergency planning, security and business continuity. The RUSI Journal, 149(4), 26-33. Pepper, M. A. (2003). Is security management a profession? [Electronic Version], from http://www.mapdsecurity.com/pdf/pub02.pdf

Rasmussen, M. V. (2004). `It Sounds Like a Riddle': Security Studies, the War on Terror and Risk. Millennium - Journal of International Studies, 33(2), 381-395.

Reid, R. P. (2002). Waging public relations: A cornerstone of fourth-generation warfare. Journal of Information Warfare, 1(3), 51-65.

Security Professionals' Taskforce. (2008). Outcomes of the 2008 Security Professionals' Congress. Retrieved. from.

Simonsen, E. (1996). The case for: Security management is a profession. International Journal of Risk, Security, and Crime Prevention, 1(3), 229-232.

Smith, C. L. (2001). Security science as an applied science? Australian Science Teachers' Journal, 47(2), 32-36.

Standards Australia. (2006). HB 167:2006 Security risk management. Canberra: Standards Australia.

Talbot, J., & Jakeman, M. (2008). SRMBOK: security risk management body of knowledge. Carlton South: Risk Management Institution of Australasia Ltd.

Taylor, P. M. (2002). Perception management and the 'war' against terrorism. Journal of Information Warfare, 1(3), 16-29.

The Interim Security Professionals' Taskforce. (2008a). Advancing security professionals: A discussion paper to identify key actions required to advance security professionals and their contribution to Australia. Retrieved. from.

The Interim Security Professionals Taskforce. (2008b). Codes of Ethics of Security Professional Associations and related organisations. Retrieved. from.

The Stanford Digital Forma Urbis Romae Project. (n.d.). Archaeological Glossary. Retrieved 12 March, 2010, from http://formaurbis.stanford.edu/docs/FURglossary.html

van Buuren, J. (2009). Security ethics: A thin blue-green-grey line [Electronic Version], from http://www.fsw.vu.nl/en/Images/De%20Boer%20INEX%20Paper_tcm31-69740.pdf

Wood, J., & Dupont, B. (2006). Democracy, Society and the Governance of Security. Cambridge: Cambridge University Press.

Zender, L. (2009). Security: Key ideas in criminology. Paris: Lavoisier.

Abolurin, A. (2010). Crime Control in Nigeria 1999-2010.

Adams, M. (1999). "Training Employees Partners " HR magazines pp. 65-70.

Ade Abolurin (2010): Crime Control in Nigeria 1999-2010.

Adebayo Akinade (2007): "A Handbook of Corporate and Industrial Security in Nigeria" Institute of security Nigeria

Adebayo Akinade (2012): Private Security Enterprises and Guard Force

Management, Institute of Security, Nigeria, Yaba, Lagos.

Adebayo Akinade (2012): Managerial and Operational Skills for Modern Security Practice. Institute of Security, Nigeria, Yaba, Lagos.

Adegoke, K. A. "'Designing Curricula; A Critique of Major Perspectives in University Education, the Art and Science of Education".

Aina S. (1992) "Personal management in Nigeria, a work centre approach Ikeja F. Communical.

Brisling, R. F. (1998) The Effe,ptive Security Officer Training Manual.

Care ne C "A Practical Approach to Personnel Management Port-Harcourt in Nigeria Gostack Printing and Publishing Co.

Cheffers, Mark and Pakaluk, M. (2005). Understanding Investigation Ethics. Manchaug, MA: Allen David Press.

Cohen A.R "Effective Behaviour in Organisation Cases, Concepts Student Experience 6"' Edition USA McGraw H.U

Cohen, A. R. Effective Behaviour in Organisation Cases, Concepts Student Experience 6`n Edition USA Mcgraw H.U.

Crumbley, D., Larry, Lester E., Heitger and G. Stevenson Smith (2005). Forensic and Investigative Investigation. Chicago: CCH Incorporated.

Davia, Howard R., Patrick C. Coggins, Jo h n 'Wideman, and Joseph T. Kastantin. Accountant's Guide to Fraud Detection and Control. Somerset, NJ: DiGabriele, James, ed. Forensic Investigation in Matrimonial Divorce.

Fafunwa, A. B. "New Perspectives in African Education. London Macmillian Education p. 50

FBI (2002). "Workplace: Issues in Response". VA, FBI: httpa'fwAwfl7ig(av_.stats Friedman, Jack P. (2003). Litigation Services

Handbook Case Studies: Investigation, Economic, and Financial Issues in Litigation Support Research. Hoboken, NJ:

John Wiley & Sons. Orukotan, A. F. (1999). "Basic Issues in Curriculum Development".

Goldstein, L L (1989) "Training and Development in Organisation " San Francisco, CA Jossy BASS publishers.

Graham, H. T. (1997). Human Resources Management. London. Pitman's.

Hilton, J. B. (1998). Is Security Training Getting Short Shrift in schools? Security Management. p. 102.

Holder, P. T. (1998). "Training/Awareness Defensive Tactics for the Security Profession ".

Ian O. lasser; (1999). Countering The New Terrorism, (ed.) Brace Hofan, John Arquilla, David Ronfeldt, Michelle Zanini.

Nicholsm, L.G (1997): "Instructor Development Training a Guide for Security Law Enforcement ", Boston M.A Butterworth Heinemann

Ogundipe, T. O. and Akinade, A. (2012). Managing Emergency to Terrorism, Human Crises and Drug Abuse for safety. Institute of Security Nigeria.

Oliver, A. F. (1965). "Curriculum Improvement; a Guide to Problems, Principle and Procedures Newton Dodd. Mead abd co. in Onwuka, U. (1981).

Onashile Y. (2008). Scientific Criminal Investigation, Detection and Prosecution. Institute of Security Nigeria.

Pastor, J. (2006). Terrorism and Public Safety Policing Cd Rom 90 min. Protection Officer Training Manual 6th Edition,

"International Foundations for Protection Officer" Saudi J. Davies and Ronald R. Minion (ed): "Security Supervision Theory and Practice of Asset Protection" 2nd Edition.

Robinson D.G and Robinson J.C "Performance Consulting Moving Beyond Training Sib Francisco Bennett Koehler Publisher.

Rome, T. L. (2009). "How to Assess the Safety and Security of your Urban centres". www.trialewwirrowe.com

Woolcut, L. A. and Rose C. A. (1979). "Business Administration. London Holton Education Publication Ltd.

Yomi Onashile (2008). Scientific Criminal Investigation, Detection and Prosecution" Institute of security Nigeria

SCIENCE AND TECHNOLOGY IN SECURITY LAW AND ENFORCEMENT

CRITICAL INFRASTRUCTURE PROTECTION: RELEVANCE OF SECURITY EDUCATION STRATEGY FOR STAKEHOLDERS AND EMPLOYEES

Brigadier – General Charles Adisa Bossman fisn
Adebayo Akinade dfisn

ABSTRACT
Today, critical infrastructures have become an integral part of cyberspace and they play a vital role in supporting many of our daily activities (including travel, water and power usage, financial transactions, telecommunications, and so on). Today, the reliability, high performance, continuous operation, safety, maintenance and protection of these critical infrastructures are national priorities for many countries around the world. We explore the various vulnerabilities and threats currently present in critical infrastructures and describe protection measures that can be deployed to mitigate those threats. There is the need to explore the challenging areas such as security education strategy, employees, stakeholders, governance and security management, network design and secure communication channels, self-healing, modeling and simulation, wide-area situational awareness, forensic, and finally, trust management and privacy that must be considered to further enhance the protection of critical infrastructures in the future. The current assessment of the current state of infrastructure and related services include water and sanitation, transportation, electric power, information and communication technology are very vital to the economy of the state. There is the need to provide education and training in order to maintain continuity, effectiveness and efficiency.
The paper will discuss communication culture, awareness programmes and mobilization of the stakeholders and employees training and education to be able to address challenges of threats and vulnerabilities.
The paper will analyse security strategies to determine the roles, interests of the employees and the stakeholders in management of critical infrastructures in order to achieve enhanced effectiveness and productivity.
The paper will discuss communication culture, awareness programmes and mobilization of the stakeholders and stakeholders and employees.

Keywords: ***Critical Infrastructure, Protection, Training, Education Strategy, Stakeholders, employers and employees, productivity, efficiency and effectiveness.***

1.00 INTRODUCTION

A Critical Infrastructure (CI) consists a set of systems and assets, whether physical or virtual, so essential to the nation that any disruption of their services could have a serious impact on national security, economic well-being, public health or safety, or any combination of these. According to the EPCIP, Critical Infrastructures (CIs) can be classified as follows:

- **Energy:** energy production sources, storage and distribution (oil, gas, electricity).
- **Information, Communication Technology (ICT):** information system and net-work protection (e.g., the Internet); provision of fixed telecommunications; pro-vision of mobile telecommunication; radio communication and navigation; satellite communication; broadcasting.
- **Water:** Provision of water (e.g., dams); control of quality; stemming and control of water quantity.
- **Food and agriculture:** Food provision, safety and security.
- **Health care and public health:** Medical and hospital care; medicines, serums,

vaccines, and pharmaceuticals; bio-laboratories and bio-agents.

- **Financial systems:** banking, payment services and government financial assignment.
- **Civil administration:** government facilities and functions; armed forces; civil administration services; emergency services; postal and courier services.
- **Public, legal order and safety:** maintaining public and legal order, safety and security; administration of justice and detention.
- **Transportation systems:** road transport, rail transport, air traffic; border surveillance; inland waterways transport; ocean and short-sea shipping.
- **Chemical industry:** production and storage of dangerous substances; pipelines of dangerous goods.
- **Nuclear industry:** production and storage of nuclear substances.
- **Space:** Communication and research.
- Research facilities.
- **National Monuments and Icons:** monuments, physical structures, objects or geo-graphical places that are acknowledged as representing national culture, or have a religious or historical importance.
- **Commercial Facilities:** commercial centers, office buildings, sports stadiums, any other place that can accommodate a large number of people.
- **Critical Manufacturing**:
  Transformation of materials into goods. This includes all the processes involved in manufacturing and transportation equipment.
- **Defense Industry Base:** production facilities of military resources (e.g., weapons, aircraft or ships) and maintenance of essential services (e.g., communication) to protect a nation.

The aforementioned sectors together with their Critical Infrastructures (CIs) are somehow connected to each other, creating a special interdependence relationship. This relationship means that a CI could require and depend on the services from another Critical Infrastructure (CI) to work properly, and the latter might also need the output from the first infrastructure. This interdependence relationship could trigger a cascading effect when disruptions of services and functionalities appear within a Critical Infrastructure (CI). ***Rinaldiet. al.*** concretely identified and analyzed up to four types of relationships: **physical, geographic**, **cyber and logical stakeholders, employers and employee relationship**. A physical interdependency refers to a dependency on receiving resources or raw material from other infrastructures.

A geographic interdependency exists when multiple infrastructures share a close spatial proximity, and any problem located in one of them can reach the other Critical Infrastructures (CIs). A cyber interdependency is attributed to the existing dependencies in communication systems and their information. Logical corresponds to those systems, actions or decisions that connect an agent of one infrastructure to another agent belonging to another infrastructure which does not have a direct link through physical, geographic and cyber connections (e.g., bureaucratic or political decisions). Obtaining, employing and retaining suitable security personnel that would contribute to the effectiveness, efficiency and productivity of service to be rendering in operations of critical infrastructure.

The roles of all the stakeholders are very paramount in order to have infrastructure which will be very beneficial to the society. There employees and stakeholders need to be trained and attain the right education in order

to address the threats, vulnerabilities and risks to the critical infrastructure.

2.00 VULNERABILITIES AND THREATS INVOLVING SECURITY MEASURES

Threats in Critical Infrastructures (CIs) are mainly caused by existing vulnerabilities and threat resources that can be exploited to produce unplanned changes in the service offered and a deviation from their normal behavior. These faults can be classified in to two categories: **internal and external faults**.

An internal fault corresponds to anomalous changes originating within the system. An external fault is related to those interactions that originate from outside the system, such as natural phenomena, malicious actions or accidents. Irrespective of the cause, any fault within the system can then create an internal effect that can collapse essential services and activities for the control. For example, an attack on a sensor node may cause errors that may affect the operations of other essential resources for the control, such as RTUs. If this occurs, the central system will then be unable to receive sensitive information from substations, becoming a system blind to the real states of the system under control. This situation can also occur when communication links stop functioning or are compromised by malicious entities, leaving critical areas and their services unprotected.

It is also important to consider the level of dependence among resources or components of a system, the segregation of functionalities and services. This means that when one component presents a particular anomaly, the result may take on a progressive effect that may change its normal behavior, which may result in a crisis situation. When the effect enters into cascading mode, the entire system and its services may also become affected, with a high probability of reaching other Critical Infrastructures (CIs) and their services. When these adverse situations occur, it is of paramount importance to be aware of four main factors: the scope of the effect, its magnitude, propagation and recovery. The first factor contributes to the loss/unavailability of an element and its impact within society which could be rated according to the geographic coverage; i.e., international, national, provincial/territorial, or local. The magnitude of the effect is related to the degree (minor, moderate or major) of the loss according to the public, economic, environmental, interdependency, and political impact. For the latter two factors, time is an essential parameter to measure the criticality of a situation because it determines at what point the loss of an element could have a serious effect; and at what point it would be possible to recover the functionality of the entire affected system.

Many of these threats are caused by the adaptation of the current Critical Infrastructures (ICTs) for control tasks and operations of critical services, such as the Internet and wireless communication technologies. The reason is quite simple. The technological introduction is simultaneously increasing architectural complexities, and adding vulnerabilities, security risks and interoperability issues. All of these aspects will be thoroughly discussed in the following section.

3.00 CHALLENGING AREAS FOR THE PROTECTION FOR CRITICAL CONTEXTS

In this section we highlight the current highest priority security areas that should be properly addressed to build a secure and sustainable future. In particular, we discuss the following challenging areas of security for protecting critical environments: *governance and security management, robust network design and secure communication channels, self-healing; modeling and simulation, Wide-Area Situational Awareness (WASA), forensic and learning, trust management and privacy*, training, education strategy and stakeholders and employees.

Governance and Security Management

To use resources and assets efficiently the system must be under the control of a suitable governance and security management. Governance is concerned with the set of security controls (i.e., actions) used to govern an organization. These controls are defined within security policies, standards, best

practices or recommendations. In particular, a security policy contributes to a set of action plans agreed or chosen by an organization and it is the means by which security requirements must be properly specified in order to enforce security controls and management.

Security controls and their abstractions are in charge of regulating the overall behavior of the entire system made up of physical and virtual entities. These entities can be human entities (e.g., staff members, providers, customers, etc.) or HW/SW entities (e.g., applications, services, resources, objects, and other stakeholders). For interoperability between entities, a set of behaviors needs to be specified according to the type of application domain and its criticality, the existing interdependencies between organizations and resources, the information architecture and its coexistence with engineering systems, information management, associated risks. Important issues that must be addressed by security controls include: *where, what, how and when an action can change the functionality of a part of the system, and who should do it.*

Controls can be categorized into a set of sub-controls which are described below. As these sub-controls are rather general, we further classify them into two categories: organizational security sub-control and operational sub-control. Both categories are defined as follows:

- ***Organizational security sub-controls*****:** this category refers to all those security sub-controls related to the organizational management (both physical and cyber) of the entire system. These sub-controls include security policy, organizational security, personnel security, physical and environmental security, strategic planning, security awareness and training, monitoring and reviewing control system security policy (review security compliance according to the security policies), risk management and assessment, and security program management.
- ***Operational sub-control*****:** this category comprises all those security sub-controls that allow a system to perform a set of activities (e.g., operational control or sensitive information management) securely. Within this classification, we include system and services acquisition (e.g., allocation or acquisition of control system assets, software and services), configuration management, information and document management, system development and maintenance, system and communication protection, incident management and response, system and information integrity, access control, audit and accountability, and media protection.

4.00 SECURITY EDUCATION FOR ENHANCED PERFORMANCE AND PRODUCTIVITY

At organisational level *Security Performance comprises the following three basic outputs:*

Effectiveness, Efficiency and Security Personnel Satisfaction

Obtaining, employing and retaining suitable security personnel that would contribute to the effectiveness and (accomplishment of the tasks) and the efficiency (best possible utilisation of resources) of the security tasks and at the same time security workers to be satisfied with their work and their lives is costly and requires considerable effort. Therefore, the employer of security has a very strong vested interest in ensuring that these human resources are utilised as effectively as possible. There is convincing evidence that some employee or personnel security are falling far short in making effective use of all the people they employ. To do this, the employer has to recognise that people are its most valuable asset. They are not simply another factor of production for the achievement of short-term objectives. It should also be recognised that security personnel can become a reservoir of knowledge and skills, which must be nurtured and developed for the survival and future growth of the employer's business in the constantly changing and increasingly complex

security industry environment. Experience from some security organisations suggests that investments in people have resulted in substantial gains towards the achievement of the business strategic objectives. There is no need to overemphasize the importance of **"Getting the right people and getting the people right" but** defining these twin concepts is a step further towards achieving increased security performance through people. ***"Getting the right people"*** means planned recruitment processes, which provide the security business with the best available talent, consistent with the needs of the security business and its capacity to make full use of those recruited. ***"Getting the people right"*** implies consistent policies and practices in training, retraining, educating and developing security staff and involving them as "partners" in the business rather than as functionaries whose roles are restricted to obeying instructions.

It is obvious that **"Getting the people right"** implies two categories of human resource policies and practices. The first category is related to learning processes and the second to security personnel motivation. **However, it is important to point out that the provision of opportunity for appropriate training, education and development is one of the proven strategies for security workforce motivation.** More often than not the terms **"Training"** and **"Education"** are used as synonyms and there is also some confusion as to what actually the term **"Personal Development"** implies. For this reason, the first appropriate step in understanding the basic training theory upon which security workforce training should be best practiced is to highlight the definitions of these terms. The common denominator of these three terms is learning. Consequently, the understanding of the learning process is also a fundamental prerequisite for those responsible in "getting people right" in security organisations. *Training is a learning process in which learning opportunities and experiences are designed and implemented, which aim in developing the knowledge, skills and attitudes related to the present job of the learner.*

Training is necessary to achieve improvements in work performance, particularly when the employer invest in new equipment, introduce new work procedures or redesign the workplace. Training takes place at a specific time and place; it is usually vocationally relevant and limited to specific aims and objectives.

There are many examples of this particular activity area of Human Resources Development (HRD) either at security, enterprise, national or international level. Security training institutes all over the world offer on a routine or tailor-made basis specific job-related training both at management.

Education *is a learning process that prepares people for a future job that may arise.* It is important to recognise that immediate increased performance cannot be expected when education is used as a HRD intervention. Education takes place over a substantial but finite period of time, usually, leads to a qualification and may result in leading you to a new career direction. However, education has been correctly recognised by many stakeholders in the security industry as an important investment for the long-term future.

Personal Development (or self-development)*,* which is initiated by the individual, is a lifelong learning process of nurturing, shaping and improving an individual's skills, knowledge and interests to ensure their maximum effectiveness and adaptability and to minimise the obsolescence of their knowledge and skills and their chances of redundancy. Personal development is not job-related. Although there may be some indirect benefits, personal development is not directly related to productivity. Hence, it would be prudent to exclude personal development as a means of achieving productivity improvement. Personal development does not necessarily imply upward movement; rather, it is about enabling individuals to improve and use their full potential at each career stage. However, any support provided by the employer to individual security employees for self-development is likely to contribute to

employee satisfaction and generate more motivation.

The Learning Process

Since training (as well as education) is essentially a learning process, all those involved in security training need to have an understanding of learning and what needs to be taken into consideration in the design and provision of training in the security sector. The main questions to be discussed are what learning is and how people learn. There is a general consensus about the first question but much more debate about the second.

"Learning" may be defined as a permanent change of behaviour, which occurs as a result of the influence of external, environmental stimuli on the inherent, genetic disposition of the individual.

For the purpose of training a similar but more specific and simple definition of "Learning" is frequently used, which is as follows:

"Learning" is a permanent change in behaviour that comes about as a result of a planned learning experience. (In simple terms training could be defined as the design and implementation of effective learning experiences).

In the context of training, it is useful to consider learning and behaviour change in three types of behaviour, cognitive (knowledge), psychomotor (skills) and affective (attitudes) needed for effective performance.

5.00 EFFICIENCY AND EFFECTIVENESS OF SECURITY TRAINING ON JOB PERFORMANCE

The measurement of security job performance is most difficult. One should not confuse efficiency with effectiveness. A security department may be highly efficient, but most ineffective in accomplishing the goals of security operation **(Akinade, A., 2012).**

The greatest improvement in security efficiency will come about, not by applications of computers to security deployment, not because more fleet patrol vehicle has been engineered, and not due to new buildings. The greatest improvement in security department efficiency will ensure the very best of talent available from the nation's man power pool, educating and training it to the limit of its capacity, and moving it up through the ranks as quickly as it is able to accept and discharge its responsibility. This talent will bring undreamed increased in efficiency - but with it, the greatest of headaches - for it will be merciless in eliminating archaic and poor attitude and practices, demanding the utmost of dedication and production of all members of the security team and mandating professional example in all aspects of the service. **(Akinade, A., 2012).**

This is not to depreciate those highly motivated security professionals who are currently exemplifying the finest ideals of service. This is to say that there is so great a need of them in the security service today that we must make maximum effort to recruit more and more men and women of the greatest capacity and character if we are to have impressive increases in efficiency. Certainly, as we approach the area of efficiency; we can identify major security goals: the prevention of crime and disorder, the preservation of peace; and the protection of life and property, and individual freedom.

And, certainly, we can identify major security methods: crime prevention: regulation of non-criminal conduct; provision of service; and protection of individual freedom. And, certainly, we can identify the major line, staff, auxiliary and special activities. Yet a variety of opinion differs according to the level of service. Certainly, we can identify major criteria of goal accomplishment: the absence of crime, disorder, congestion, accidents, and conflict within the community; adequate rates of arrest, clearance, property recovered, and successful prosecution; minimum employee ratios and minimum per capital cost consistent with adequate performance; services and personnel.

A variety of opinions lays that to such yardsticks, depending upon the level of service and company values.

Security training should also concentrate on the behaviour of the personnel. Morality is therefore concerned with standards or principles of good behaviour. There is a general agreement, for example, the human being ought to be honest, kind and helpful to one another. These are matters of morality. Private morality deals with those values which affect the individuals concerned. Public morality deals with those values which affect the society as a whole.

Enforcement of morals could, therefore be defined as the use of law to make effective some standards of good behaviour. This could be done either by imposing duties or by limiting liberties. Moral rules according to **C.S Lewis**; are directions for the running of the human machine. Every moral rule is there to prevent breakdown, or strain, or a friction, in the running of the machine. That is why these at first seem to be constantly interfering with our natural inclination.

6.00 TRAINING AND EDUCATION IN OPERATION AND MANAGEMENT OF CRITICAL INFRASTRUCTURE

Critical infrastructure training and education programmes are diffuse, diverse, desperate and complex. The training programmes promote awareness of security and protection issues throughout the critical infrastructure sectors. The training and capacity building programme should meet the security awareness and practice needs of anti-terrorism workforce and criminal intelligence that is diverse **(Abolurin, A., 2010)**

Ralph F. Brisling (1998) advocates for the use of training manual to enhance training and professionalism, improve service, reduce turmoil and minimise liability. He recommended the use of practical exercise demonstrating how to handle disruptive people, prepare for emergencies and design patrol procedures as well as advise on testifying in court, writing reports and coping with internal threats.

Training and education programmes in critical infrastructure sectors are designed to offer a thorough coverage of the techniques, strategies and skills available for awareness and acquisition. Critical infrastructures, the objective of the programme are to share experience, knowledge and skills through workshop style experience combined with real life examples and to gain the tools and techniques necessary to resolve even the most complex cases of terrorism, application of criminal intelligence techniques and faults which could disrupt operations of critical infrastructure protection. The challenging fully packed training programme will provide participants with all theories and practical tools needed to identify, investigate and respond to terrorism in the nation. Training and education programme gives practical advice and guidance on how to pursue the perpetrator identified as a result of counter terrorism techniques and devices.

Three-dimensional focus on the importance of careful planning and research, can be provided with a framework to enable the participants develop plans and tools to adapt their thinking to that of top-class counter terrorism professionals. The professionals should be able to understand how to develop critical infrastructure protection strategies to prevent terrorism from occurring and recognise the red flags of terrorism and extremism in the country.

Security professionals now place an unprecedented emphasis on risk assessment and mitigation of various threats, vulnerabilities and risks are shifting the current community policing model to one that emphasis tactical methods, technology and alternative service provider. The new public safety model entails wide spread employment of private security officers in public areas such as business districts, residential and industrial communities and critical infrastructure sectors.

James Paster (2006) provides cutting edge analysis demonstrating continued expansion of private security and policy agencies will increasingly perform coordinated work

sharing within public environments and promotion of the principle of community policing in security practice.

Carl Roper (2005) and some security experts emphasized the need for quality security awareness training, they maintained that while technology and corporate dynamics have changed and developed, the need for security awareness training has remained. The book covers security training at all levels. It addresses the theories of sound security training and awareness, and then shows the readers how to put the theories into practices. An important requirement of security agency charged with responsibility of counter terrorism is the availability of well-trained personnel. This is a major pre requisite for operational effectiveness. The agency therefore should place much emphasis on training and education to ensure operational readiness at all time.

It must be mainly responsible for the implementation of counter terrorism policies. It is to the credit of such security agency. This could be achieved by using all available training facilities in the country and at the same time expansion. There is the need to examine training and counter terrorism efforts and measures to combat the intellectual and ideological justification for violent extremism. The primary objective of this training is to engage and combat an ideology on counter terrorism policy that seeks to address - the underlying factors that have facilitated extremism in the hope of preventing further radical violence. Prevention programmes are difficult to evaluate and much more time will be required to accurately measure their effectiveness.

Larry Gene Nicholson (1997) examined in his book that as the need for professional security increases, so too does the need for professionally trained personnel. He explained the need for an organised approach to developing effective security and law enforcement training programmes.

Security threats, vulnerabilities and risks in critical infrastructures training and education programmes are varied by numerous security agencies and departments. Each of the relevant security agencies should provide specific counter terrorism training and education targeted to categories of stakeholder's employees and employers. Training recipients include federal, state, local government personnel and private and public critical infrastructure personnel. The programme should train individuals to prepare for, respond to and recover from terrorist attacks and detection of serious faults. Most of these federal security agencies and departments should provide training in conjunction with private and public educational institutions, federal laboratories and research and development centres.

Developing and maintaining an effective security and resilience posture depends on the security and resilience expertise diligence and the level of security and protection education and training of the employees of the organisation workforce.

There is the need to begin with explanation of myriads of issues associated with the fielding of a security force and the types of education and tripping that can be used to determine the best coverage options available.

A security and safety force planning flow chart clarifies the decision points leading to a deployment of dedicated security force. The pros and cons of engaging security consultants or security constructor will be discussed, followed by commentary on the importance of involvement of the organisation, non-security personnel in the security efforts.

Security Forces

The costs associated with deploying personnels are the most expensive security countermeasure a security department can undertake. The labour costs associated with the company's operating budget for security can exceed 90 to 92% of total annual expenditure. However, depending on the threats and unresolved vulnerabilities facing the organisation, security personnel are often the most critical and significant resource available to reduce security related risk.

Security personnel provide a vital capability for which there is no substitution-the ability to comprehend and apply reason. Security personnel can perceive the nature of a threat and recognise ongoing aggressor tactics. When adequately armed or reinforced, they can repel or overcome the use of deadly force by responding with equal or greater force to neutralize the threat or activity. This factor alone is predominating in both the internal security and public safety context. In the absence of a response; aggressors or criminals would quickly disregard other security countermeasures as irrelevant.

Deciding on the necessity for security personnel or the extent to which forces should be deployed can be a significant challenge for security decision makers. The answers depend on the threats facing the agency and issues such as size, population served, and operating locale. For example, transportation systems operating in high-density population areas probably are at higher risk of attack than more rural systems. Other external factors can affect security personnel decisions (e.g., the availability of public safety response personnel in the operating area, what users or customers expect to see in terms of security, or whether other organisations in the industry use security personnel). Internal factors such as the agency's history of deploying security forces or whether the organisational culture is tolerant of security restrictions will also have its bearing. In general, transportation agency decision makers have an initial-spend or no spend-hurdle to clear in thinking about security personnel deployment. To do so will require significant inter-action with local authorities to establish the level of protection and response to security incidents that can be expected.

Security Experts, Consultants, and Contractors

There is the need to use security professionals to help in certain aspects of risk assessment, security planning, and countermeasures identification. It is specifically necessary that security consultants be contracted to assist in the performance of security vulnerability assessment (SVA) and security plan development. Obtaining professional help in security workforce planning may also be appropriate. Security contractors should be retained to assist in security systems integration, particularly in connection with the selection and implementation of hardware and electronics such as intrusion detection, alarm systems, access control, and CCTV.

Frequently, an organisation will hesitate to formalize a consulting arrangement with a security practitioner or firm; this hesitancy does not always make good business sense. Even the most professional in-house security departments, as expert as they may be in all phases of security risk management, processes and procedures, and security technologies, use independent outside contractors. Competent security consultants are available to perform research, analyse conditions, and develop comprehensive security programmes that can reduce the risks, associated with conducting transportation operations. Of course, this assumes that the agency has identified the right consultant or consulting service.

The two main factors to be evaluated when selecting professional security consulting assistance are:

- Review of the documented qualifications of the security firm and
- The backgrounds of the individuals who will perform the security work.

Ideally, the agency will be able to identify a security firm with a successful record of past contracted employments performing work in the specific transportation sector and discipline (e.g., rail, port, airport, pipeline, highway, or transit). In addition, the security firm's leading experts will be available and, on the team, assigned to conduct the security work contemplated. Hiring an independent security consultant is not the same as; accepting security "recommendations" from a manufacturer or retailer's representative. Independent consultants can be called on to provide objective opinions without bias or predetermination. Salespersons, especially those with high technology products, are

usually limited in approach and biased toward the company they' work for. Out of loyalty to their companies and sometimes their commissions, the sales pitches of security contractors may propose security staffing or technology that does not fit the risk profile or operating environment of the agency.

Overemphasis on guards, alarms, or surveillance systems can drain operating and capital budgets unnecessarily when the proper solution is the integrated - balancing of security policy and procedure with the other countermeasures in the agency's toolkit.

Security Committees and. Employee Watch Programmes

As with safety, security in critical infrastructure sectors is a "top-down" organisational activity. This is because executives, by necessity, must support cross-disciplinary functions in order for the activities to succeed. By lending support to important agency functions, leadership drives the prioritization of work to comport with the direction provided. Unfortunately, security as a function within an agency is often deemphasized until an incident occurs. Managers, many times because of their lack of familiarity with the subject matter, can be reluctant to broach the issue of security. Then when an incident happens, impromptu crisis thinking can intrude: on disciplined managerial decision-making, causing "knee jerk" reactions that defeat security planning and preparedness. To overcome this tendency, senior management of an organisation must be active in determining the course of the security related activities of the agency. It is recommended that the chief executive establish a senior advisory group consisting of executives from various departments who have designated oversight authority for system wide security. This senior committee should meet regularly to establish direction and develop strategic-level security policies and guidelines. The agency should also involve front-line and mid-management level employees in security.

Representative individuals from across the agency should be selected to serve as security coordinators and as participants in security committees. Where the agency maintains a dedicated security force, department coordinators should be responsible for day-to-day security interface and liaison. In those agencies without a dedicated security force, a committee of department security coordinators should be empowered with the authority to manage security activities system wide. The key objectives of programme coordination are as follows:

- Deploy a broad-based systemwide security management process that identifies, tracks, and responds to all security threats, vulnerabilities, and occurrences;
- Maintain a workplace where security incidents are routinely reported and contributions to improve security are received from every staff and operating department; and
- Ensure that front-line and mid-management employees promote security awareness and communications throughout the organisation.

Employee watch programmes have long been recognised as an important security tool available to employers. However, most of these programmes fail or are moderately effective because of a lack of guidance and support. It is not sufficient for an agency to enlist participants and then send them out to "do security." The agency's security planners must work aggressively to define the security awareness roles, responsibilities, and criteria for such programmes. This includes a basic security issues assessment, formulation of either step-by-step implementation plans or fresh start "invigorators," and creation of calendar initiatives designed to keep employee watch participants actively engaged in security. Participants should also receive priority enrolment for attendance at security training.

Security Training in Critical Infrastructure Protection Management

The employees of organisations are a critical resource for maintaining a safe and secure operating environment. They represent an

omnipresent team of experienced people who are knowledgeable and insightful about the work of the agency, as well as the operating norms and environmental conditions that affect the workplace day to day. Because of their continued presence in and on agency properties or conveyances employees are uniquely positioned to identify issues, problems, and deviations from what is usual.

In security, this capability takes the form of recognising suspicious activities and identifying dangerous or hazardous conditions. For example, in response to a bomb threat in an administrative area, an office worker is better equipped to find a suspicious item or package in his workplace than first responders who are unfamiliar with the surroundings. Employees are also at the forefront of organisational activities, performing work in stations, on vehicles, in plants and warehouses, and on roadways and rights of way. As such, they are often the first to observe that something is wrong. But transportation agencies cannot assume that employees will focus on security issues without training. Employees need to receive security awareness orientation to prepare them for their security roles. Thereafter, employees must be able to practice what they have been taught to reinforce a security awareness culture at the agency. Establishing a security culture for all employees is mandatory for maximizing the security effectiveness of an organisation.

The responsibility for development, oversight, and enhancement of security awareness programmes and activities should be given to a specific individual or function. This assignment can be full- or part-time, depending on agency size and operations balanced against security risk. But similar to safety, regardless of size or risk, transportation agencies at minimum should implement a security awareness programme that enables all personnel to contribute to the security of the operating environment.

TRAINING, CONFERENCES, ADVISORY SERVICES

In order to ensure efficient and reliable exchange of information between Critical Infrastructure system participants, it is necessary to support activities of an educational nature undertaken under the critical infrastructure protection forums. Such activities cover:

a) provision of mutual substantive support (as advisory services and training) by public administration entities and CI operators,
b) participation of critical infrastructure operators and administration entities in practical exercises in the
c) field of critical infrastructure protection,
d) participation of_critical infrastructure operators and administration entities in conferences in the field of critical infrastructure protection,
e) integration of communities responsible for critical infrastructure protection.

Practical exercises falling within the scope of protection of critical infrastructure

Practical exercises form the most effective form of training. They facilitate a complex process of gaining and maintenance of a high level of knowledge and practical trained skills. They are aimed at development, establishment and mastering of habits necessary in the process of task fulfilment management by functional persons and human resources teams at all levels. They create conditions for apt selection of effective forms and methods of activities in various situations, mainly while taking and implementing certain decisions and managing subordinate units. They will be conducted on all levels of public administration and in the private sector.

Practical exercises are aimed to:

1) Practically verify the correctness of operation of the critical infrastructure protection system,
2) Prepare persons to whom performance of tasks has been entrusted within the framework of critical infrastructure protection, as well as persons participating in the fulfillment of those tasks,

3) develop skills of cooperation of authorities and organizational units ensuring critical infrastructure security with relevant forces, institutions and governmental administration authorities,
4) Raise awareness about threats and adequate methods of reacting to them by persons taking part in practical exercises.

Practical exercises falling within the scope of CI protection may take the form of:
1) Readiness tests (checking the time of reaction);
2) Standard operating procedures tests (e.g. information exchange procedures);
3) table-top exercises;
4) practical exercises;
5) decision-taking games.

Exercises are participated in by:
1) Persons who hold managerial positions in public administration, in particular:
   a) ministers, permanent secretaries, persons who are central a thorities of governmental administration or their deputies, of departments or their deputies, managers of bureaus in offices servicing ministers, central authorities and other state organizational units performing tasks falling within the scope of critical infrastructure protection, as well as directors of departments in provincial offices or their deputies;
   b) state permanent secretaries, local government, chairman, and their subordinate forces, inspections and services and forces, inspections and services supervised by them;
   c) Directors of departments or their deputies, managers of bureaus in offices servicing ministers, central authorities and other state organizational units performing tasks falling within the scope of critical infrastructure protection, as well as directors of department in provincial offices or their deputies.
2) employees of organizational units managed by the persons holding the positions referred to in point 1 letter c, employed in the positions connected with critical infrastructure protection.

7.00 STRATEGIC SECURITY MODELS FOR STAKEHOLDERS AND LEADERSHIP IN CRITICAL INFRASTRUCTURE PROTECTION

Concept of Strategy for Security Stakeholders

Security Strategy should be based on the understanding of how security can be used to involve and facilitate the key players in carrying out different aspects of security management in a more effective way particularly in critical infrastructure sector.

In the management literature, the most relevant, theory is the stakeholder theory. In his landmark work "Strategic Management: A stakeholder approach", ***Freeman (1984)*** proposed the use of stakeholder analysis for the guidance of strategy making. Therefore, the first object of this paper is to conduct a stakeholder analysis in security management in critical infrastructure sector in order to identify the stakeholders, their interests, roles and relationships with each other. Based on the analysis, the next objective is to find out the optimal strategy to involve all stakeholders in security management in critical infrastructure sector. Based on the discussion of their interests, roles, and relationships, these factors can be considered as the needs for security strategy enable stakeholders to share experiences and information with each other in critical infrastructure sector.

Security information and intelligence have been widely used in corporate settings as the primary method for organising and discovering corporate resources. Security management for the purpose of enabling all stakeholders to participate in its different aspects include: (1) security assessment, (2) security control, and (3) security communication in critical infrastructure sector.

In their well-cited paper, ***Donaldson and Preston (1995)*** classified the concepts of

stakeholder theory, tested its validity and elaborated its implications. In the context of corporation, stakeholders are persons or groups with - legitimate interests in procedural and/or substantive aspects of corporate activity which can be identified by their legitimate and intrinsic interests in the corporation.

Security management can be regarded as an activity that involves multiple groups. Stakeholders in security management are groups with legitimate and intrinsic interests in security and safety in critical infrastructure protection.

Freeman (1984) suggested that to be a stakeholder, the group should be affected and be able to affect the achievement of the organisation's objectives. Thus, the following two conditions are to be fulfilled in order to be a stakeholder in security management:

(1) Directly affected by criminal and terrorist attacks on security systems
(2) Contribute significantly to the war against criminality and terrorism.

If the first condition is met, it means that the group has intrinsic interests and if the second condition is met, it means that the group has the legitimate interests. Not all groups that have intrinsic interest are stakeholders because they may not have the legitimate interest, such as the criminal or terrorist groups.

Also, not all groups that have the legitimate interest have the intrinsic interest, such as the security equipment supplier. Only when a group meets both conditions, it can be regarded as the stakeholder in security management.

Though terrorisms may take many forms and is hard to define, terrorist attacks share the following factors, in common:

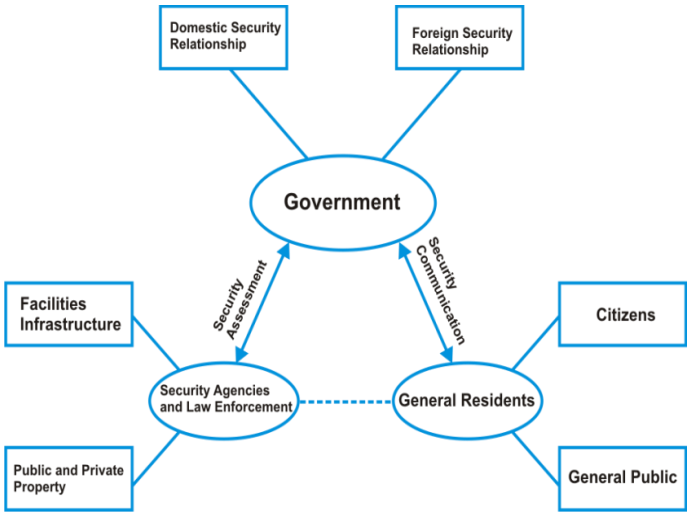
(1) are politically motivated,
(2) target non-military targets and civilians,
(3) intend to instill fearful state of mind in the audience.

The physical targets of terrorist and criminal attacks on civilian and- security systems are community facilities, infrastructures building premises and people in them. The psychological target, on the other hand, is general public and government because the terrorists influence the political decisions of the government through influencing people's thoughts and feelings.

In public security management, the government makes security-related policies to provide financial and technical support and supervise the progress in enhancing security measures. Though the public does not play a formal role in the current security management, it can make a great contribution. Public can help detect criminal and terrorist efforts by reporting suspicious persons and activities. The general public is also a source of intelligence on suspects that live and work among them. Thus, the government, security agencies and the general public can contribute significantly to public and private security management.

Because the government security agencies and the general public have both intrinsic and legitimate interests in security and safety, they are the stakeholders of security operations and management particularly in critical infrastructure protection.

There is a triangle of bilateral relationships among them as indicated below. A formal relationship (indicated by the solid line) between these two and the public in security management, including: security assessment, security control and security communication.



8.00 CURRENT RELATIONSHIPS AMONG STAKEHOLDERS IN CRITICAL INFRASTRUCTURE PROTECTION

The stakeholders in critical infrastructure, including employees' employers, contractors, visitors, consultant vandalism, criminals and terrorists. Security assessment is the proactive measures to identify and nullify potential security breaches and threats before the criminals and terrorists invade urban communities and security systems. Security assessment is mainly between the government and security agencies and law enforcement agencies and it has the following two major tasks to perform:

(1) to identify security weaknesses in security systems so that they can be enhanced before criminals and terrorist can exploit them.

(2) to identify criminal terrorist suspects so that they can be kept out from the urban communities and facilities. Security control is the reactive measure to detect and counteract criminals and terrorist efforts inside the urban communities and facilities.

Currently, security control is mainly between security agencies and the general public, they detect any suspicious activities and persons with suspicious character or behaviour in the community. They take appropriate steps to stop any malicious activities.

Security communication is the post-active measure which offset the influence of criminal or terrorists' attacks on the community or facilities.

The final target of criminals and terrorist attacks is people's psychology which is an important aspect of war or counteraction against crime and terrorism. This establishes healthy public perceptions through proper risk communication.

Currently, security communication is mainly between government and the general public. The government guides the public perceptions on community security and hears the feedback from the public.

The proactive security assessment, reactive security control and post-active security communications are achieved through the bilateral interactions among the stakeholders. The one-on-one interactions in bilateral relationships are relatively easy to handle. However, there is no active involvement of stakeholders in each aspect of security management. If all three stakeholders can participate in security assessment, control and communication, it is expected that the objective of security management can be accomplished more effectively. However, that requires the three stakeholders to be able to share information and intelligence with each other.

In organizational settings, the information and intelligence approach along different groups within and across the systems or enterprises to share information or intelligence system for better coordination and cooperation among them in critical infrastructure sectors.

In security management, the employment of such an approach will enable government, security agencies and general public to contribute and access information needed for security assessment, control, and perception. This security strategy will lead to change in the current security systems by involving all the three stakeholders in security management.

In terms of security assessment, the involvement of the general public may help the government, the public and private security agencies to identify potential security weaknesses, threats, terrorist and criminal suspects. To allocate limited resources to enhance the security measures, the government usually quantities risks by identifying the weaknesses, evaluating the vulnerability and estimating the consequences.

However, criminal and terrorists' attacks are relatively infrequent but the consequences can be extremely severe. Thus, it is almost impossible to objectively quantify risks of criminal and terrorist attacks in communities and security systems based on historical data. Involving the public through the information or intelligence approach allows people to report any breaches that they observe and rank their vulnerability and consequences. The public can also be a source or intelligence to identify criminal and terrorist suspects, through the information. The public may be encouraged to track report such behaviour and any suspicious activities so that the government could trace down the suspects.

In terms of security control, the involvement can help the security agencies and public detect and stop criminal and terrorist activities within the community and facilities. Information and intelligence approach, by the security agencies and the public encourages the government analyse the information and quickly share it with the intelligence community and security agencies.

In this way, the security agencies and the public will be better informed about the nature and scope of security threats, breaches and attacks and react in a proper manner. In emergency cases, the government can mobilize forces to help the security agencies and the public to fight with the criminals and terrorists and such actions require timely coordination among those who are involved.
In terms of security communication, the information and intelligence approach can provide a means for better risk perception of stakeholders. It has been found that people's perceptions of the danger from terrorists and criminal attacks are often amplified after major criminal or terrorists' attack.

9.00 STRATEGIC SECURITY MODEL (SSM)

Strategy is at the core of the strategic security model (SSM) system. Strategy constitutes the broad priorities that an organisation plans to pursue in order to fulfill its mission. The priorities must be consistent with the organisation's unique situation and fit with one another in an effort to respond effectively to challenges and opportunities. The strategic security leadership (SSL) system centred on expansive security concept which must overcome the organisational inertia that tends to immobilize virtually any change program. Strategic security is a development model for the organisations for strategic level leadership. Potential signifies a dimension reflecting total personal capabilities in the development of a learning organisation. According to the constructivist conception of learning, the process in which the potential is utilised, or enlarged is merely infra-personal.

The nisus of the model is the strategic security vision of the organisation. Without a clear understanding of the strategic vision, development of indicators for the SSM is fruitless. All perspectives, must relate to the strategic vision, and each perspective relates to the others through the central vision driving the organisation. As tactics are described, the data collected in the SSM reflects the organisation's progress toward achieving the

goals delineated by the strategic vision. A well designed SSM serves as bridges that gap between long term strategies and day-to-day action by aligning performance measures with the critical perspectives of the organisation. The SSM provides senior executives and leaders with the ability to track performance against established strategic and operational goals. The SSM takes the strategy of the organisation, converts it into a form that everyone understands, and communicates the plan and its requirements to everyone in the organisation.

Concept of Strategic Leadership

The new concept of Strategic Security Leadership (SSL) of an organisation attempts to move the emphasis of leadership from ordering and strict control of leadership that makes subordinates commit to it. Shifting the emphasis does not change the leader-centricity of decision-making and responsibility, but requires the leadership to behave with increasing flexibility and emotional intelligence. The requirements are justified with the fact that with the commitment of the subordinates the situational sensitivity and efficiency of the entire organisation improves.

Leadership is a non-hierarchical concept. Thus, SSL should be found throughout the organisation, as should acknowledgment of the significance of encouraging leadership behaviour at all levels of an organisation. The mission of key security leadership is the maintenance and modification of culture to an organisation's changing environment. The culture is based on a contingency model and consequently the role of security leaders is to be the embodiment of management the culture, because their behaviour is closely observed. It is one of the most admirable human qualities when people can identify the difference between what others say and what they do. It becomes clear that the role of a leader is to be an example of the security culture, crucial to both continuance of appropriate elements of the security culture, and equally significant in the process of constant adjustment in response to a changing external environment.

Strategic security as a high leverage mechanism requires proactivity, initiative, creativity, and ingenuity. The strategic security cluster requires a rigorous process and commitment, but its benefits worth the costs. Even if only a few of the elements of the strategic security cluster are adopted, a competitive advantage is to be gained. Best of all, much of the strategic security cluster is simple common sense: getting agreement on vision, strategy, strengths, and weaknesses; measuring essential performance numbers; and focusing not just on financial outcomes but also on the issues that will affect the future outcomes. The strategic security cluster leverages common sense into a substantial competitive advantage. Successful performances turn to indicators measuring their success. For a strategic security cluster gauge, which offers a relevant and accurate picture of an organisation's health, the organisation may leverage additional important indicators of current and future performance. A strategic security cluster measurement is not complete without strategic performance measures of stakeholders, employee and government satisfaction. These indicators often detect the warning signs of trouble early enough to take corrective action before core performance begins to suffer.

The risks of the SSM are, for example, that the commitment of the top leadership is not strong enough, huge amounts of data is collected, short term and day-to-day metrics are overemphasized and the organisation chooses the wrong indicators. Additionally, the risks include that the organisation sets unrealistic goals, and the data to be measured is difficult to collect. The organisation lacks communication, the SSM creates an enormous amount of resistance, which- change the performance to be slow and the organisation may have many overlapping systems which may be based on wrong strategy basis. The SSM responds to the challenges of security systems. However, this model may also be transferred elsewhere like state organisations which it may be adopted in the public and private security sectors. In a flexible manner, it can be used at all levels and sectors of an

organisation. It can conceptualize security at both strategic and operational levels the environment of the security organisations.

10.00 SECURITY THREATS, VULNERABILITY, AND RISK: THE SYSTEMS APPROACH IN CRITICAL INFRASTRUCTURE PROTECTION

Protection measures should be considered when new, but also conventional, technologies and information systems are being adapted to control the vast majority of our critical infrastructures. These measures should not only include traditional security mechanisms to detect and react against potential threats, but the system should be also based on intelligent mechanisms with the capability to identify vulnerabilities and faults that can be exploited by intruders.

The goal of the attacker is basically to try to bypass the security mechanisms so that once inside the system others types of threats can be launched, such as memory dump, execution of false commands to activate/deactivate critical assets, modification of state values or critical processes, etc. This paper has analyzed, on the one hand, the relevance of new technologies in control and automation tasks, and on the other hand, the motivations for the need to protect control systems when using these technologies and their information systems. Moreover, these analyses also include a study of security requirements we need to protect the control systems and the protection of the controlled critical infrastructures themselves.

We have identified several research areas that should be explored further in the future to enhance the protection of critical infrastructures. These priority research areas include governance and security management, robust network design and secure communication channels, self-healing, modeling and simulation, wide-area awareness situational, forensic and learning, trust management and privacy.

Security Director and personnel in charge of critical infrastructure must ensure that appropriate physical security measures are taken to minimize the loss of personnel, supplies, equipment, premises, facilities, infrastructures, and material through both human and natural threats. Security directors and personnel should commonly exercise those protective responsibilities through security operative and staff. The security director must coordinate with several different agencies to complete his mission of security and protection.

PROTECTIVE SYSTEMS

(a) The approach to developing protective measures for assets, facilities and people should be based on a systematic process resulting in an integrated protective system. The protective system focuses on protecting specific assets against well-defined threats to acceptable levels of protection. The system is organized in-depth and contains mutually supporting elements coordinated to prevent gaps or overlaps in responsibilities and performance.

(b) Effective protective systems integrate the following mutually supporting elements:

- Physical protective measures, including barriers, lighting, and electronic security systems.
- Procedural security measures, including procedures in place before an incident and those employed in response to an incident. These include procedures employed by asset owners and those applied by and governing the actions of guards.
- Terrorism counteraction measures that protect assets against terrorist attacks.

(c) The following determinations are made when considering system-development procedures in critical infrastructure protection:

- The resources available.
- The assets to be protected.
- The threat to those assets.
- The risk levels applicable to those assets.

- The applicable regulatory requirements for protecting the assets.
- The applicable level of protection for those assets against the threat.
- Additional vulnerabilities to the assets (based on the threat).

11.00 CONCLUSION

Policy implications for training, education and manpower development and their relevance need to be considered and the theoretical explanation need to establish whether training, education and manpower development have direct impact on improved job performance of employees who work on critical infrastructure protection.

The verification of circumstances within training, education and manpower development can enhance job performance in operations and management of critical infrastructure protection. It is noted that theoretical postulations that capacity building of employee's training and manpower development could increase efficiency in employee's performances can always be guaranteed.

Policies, procedures, instruction and documentation of training, education and manpower development must be developed to manage the implementation of the scheme. For example, policies are needed for pre-employment, assignment, recruitment of employees' tasks, training, promotion, motivation factors. Procedures are needed for reporting and responding to feedbacks. Employees' awareness and training programme, improve job performance and provide better understanding of job performance and productivity. Relevant information is needed to support policies on training, education and manpower development.

Effective training will enhance security integrity, security systems will work correctly only if they are properly designed, fabricated, installed, operated, maintained, inspected and tested. This requires a system integrity or quality assurance and maintenance programme to ensure the continued integrity of security system. A security integrity programme include requirement for written specifications for security critical materials, equipment and system; procedure to ensure they function as intended. Employee training, maintenance, inspection and testing; periodic test to challenge the security programme and quality assurance.

The training, education and manpower development programmes could focus on the following areas:

1. Coordination with other security and law enforcement agencies on counter terrorism and intelligence network to address problems relating to critical infrastructure protection.
2. Employee involvement and security awareness with the public on critical infrastructures
3. Process security information on critical infrastructures
4. Threats and risks assessment of processes on critical infrastructures
5. Management of change critical infrastructures
6. Emergency response and crisis management of critical infrastructures
7. Managing process safety critical and infrastructures security.

The capacity of training, education and manpower development to increase efficiency in employees' performance cannot always be guaranteed.

Counter terrorism on critical infrastructures: Tools and tactics used in countering terrorism are numerous and diverse, ranging from high-tech satellite surveillance systems, unmanned aerial drones and data mining software, to low-tech undercover operatives, criminal informants, and tips from suspicious neighbours. Intelligence analysts sift through mountain of data provided by these electronic and human sources to identify terrorist and their groups-controlled structure, and track down techniques are very vital to attack terrorism ***(Aldnade, A., 2012).***

Counter-terrorism is a massive global industry which takes place at various levels, ranging from local police investigation of terrorist act to invasion of countries perceived as providing cover for terrorists.

Law enforcers and military personnels carry out air strikes and raids against identified targets. During raids, authorities arrest suspects and capture documents, computers and other articles, containing organisational memoir that can be squeezed for additional intelligence about the whereabouts and impending activities of other network members.

Government agents use these data to conduct more raids and capture additional terrorists and organisational data which provide more information to be assessed, analysed and acted upon in the ongoing pursuit of the terrorists.

REFERENCES

1. C. Alcaraz, G. Fernandez and F. Carvajal, Security aspects of SCADA and DCS environments, *Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, Defense*, Springer, 120149, 2011.
2. Akinade A. (2017): "Fundamentals of Critical Infrastructure Protection. Institute of Security, Nigeria. Lagos.
3. John D. Moteff (June 10, 2015): "Critical Infrastructure Background Policy and Implementation Congressional Research Service. Critical Infrastructure Protection. Report to congressional Legislator, 17th Sept. 2014
4. C. Alcaraz, J. Lopez, J. Zhou and R. Roman, Secure SCADA framework for the protection of energy control systems, *Concurrency and Computation Practice & Experience*, vol. 23, pp. 1414-1430, 2011.
5. C. Alcaraz, R. Roman, P. Najera and J. Lopez, Security of industrial sensor network-based remote substations in the context of the Internet of things, *Ad Hoc Networks*, Elsevier, vol. 11(3), pp. 1091-1104, 2013.
6. C. Alcaraz and S. Zeadally, Critical Control System Protection in the 21st Century, *IEEE Computer*, vol. 46(4), pp. 74-83, 2013.
7. C. Alcaraz and J. Lopez, Wide-Area Situational Awareness for Critical Infrastructure Protection, *IEEE Computer*, vol. 46(4), pp. 30-37, 2013.
8. ARTEMIS, Internet of Energy for Electric Mobility, European Project, http: //www.artemis-ioe.eu/, retrieved on October 2014, 2011.
9. F. Baker and D. Meyer, RFC 6272: Internet Protocols for the Smart Grid, http: //www.ietf.org, retrieved on October 2014, 2011.
10. B. Bondi, Characteristics of scalability and their impact on Performance, *2nd International Workshop on Software and Performance* (WOSP), pp. 195203, 2000. Adebayo Akinade (2005): Managerial and Operational Skills for Modern Security Practice
11. Adebayo Akinade (2006): Security Operations, Crime Prevention and Good Governance: Pattern and Trends
12. Bassiouni, M. C. (2004): Terrorism: the Persistent Dilemma of Legitimacy Case Western Reserve, Journal of International Law
13. 36(2/3) 299-306
14. Ying Wang: Information Portals Strategy for Transportation Security Management: A StakeholderAnalysis
15. Donaldson, T. and Preston, L.E. (1995): The Stakeholder Theory
16. of the Corporation: Concepts, Evidence and Implications. The
17. Academy of Management Review 20(l),65-91.
18. Earl; M. J. (1989): Management Strategies far Information Technology: Prentice Hall, International (UK) Ltd.
19. Del Rosso Jr., Stephen J. (1995): "The Insecure State: Reflections on the State and Security in a Changing World" Daedalus, Vol.
20. 124, No. 2 (Spring) pp 175-207.
21. Aloy Ejogu (2010): "Total Involvement Management a 21" CenturyImperative".
22. Nanus, Burt (1992): "Visionary Leadership". San Francisco: Jossey-Bass Publishing.

23. Fairholm, Gilbert W.: "Leadership and the Culture of Trust".
24. Westport Comm.: Greenwood Publishing Group, Inc.
25. Covey, Richard R. (1990): "Principles Centred Leadership". New
26. York: Simon and Schister
27. Abolurin, A. (2010). Crime Control in Nigeria 1999 -2010.
28. Adams, M. (1999). "Training Employees as
29. Partners" HR magazines pp. 65-70.
30. Ade Abolurin (2010): Crime Control in Nigeria 1999-2010.
31. Adebayo Akinade (2007): "A Handbook of Corporate and Industrial Security in Nigeria" Institute of security Nigeria
32. Adebayo Akinade (2012): Private Security Enterprises and Guard Force Management. Institute of Security, Nigeria, Yaba, Lagos.
33. Adebayo Akinade (2012): Managerial and Operational Skills for Modern Security Practice. Institute of Security, Nigeria. Yaba, Lagos.
34. Adegoke, K. A. "Designing Curricula; A Critique of Major Perspectives in University Education. the Art and Science of Education".
35. Aina S. (1992) "Personal management in Nigeria_ a work centre approach Ikeja F. Communical.
36. Brisling, R. F. (1998) The Effective Security Officer Training Manual.
37. Caroline C "A Practical Approach to Personnel Management Port-Harcourt In Nigeria Gostack Printing And Publishing Co.
38. Cheffers, Mark and Pakaluk, M. (2005). Understanding Investigation Ethics. Manchaug, MA: Allen David Press.
39. Cohen A.R "Effective Behaviour in Organisation Cases, Concepts Student Experience 6`h Edition USA McGraw H.U
40. Cohen, A. R. Effective Behaviour in Organisation Cases, Concepts Student Experience 6`h Edition USA Mcgraw H.U.
41. Crumbley, D., Larry, Lester E., Heitger and G. Stevenson Smith (2005). Forensic and Investigative Investigation. Chicago: CCH Incorporated.
42. Davia, Howard R., Patrick C. Coggins, Jo h n 'Wideman, and Joseph T. Kastantin. Accountant's Guide to Fraud Detection and Control. Somerset, NJ:
43. DiGabriele, James, ed. Forensic Investigation in Matrimonial Divorce.
44. Fafunwa, A. B. "New Perspectives in African Education. London Macmillian Education p. 50
45. FBI (2002). "Workplace: Issues in Response". VA, FBI: http:/Iwwwfbi.,izov.stats
46. Friedman. Jack P. (2003). Litigation Services Handbook Case Studies: Investigation, Economic, and Financial Issues in Litigation Support Research. Hoboken, NJ:
47. John Wiley & Sons. Orukotan, A. F. (1999). "Basic Issues in Curriculum Development ".
48. Goldstein, I. L (1989) "Training and Development in Organisation" San Fransisco, CA Jossy BASS publishers.
49. Graham, H. T. (1997). Human Resources Management. London Pitman's.
50. Hilton, J. B. (1998). Is Security Training Getting Short Shrift in schools? Security Management. p. 102.
51. Holder, P. T. (1998). "Training/Awareness Defensive Tactics for the Security Profession ".
52. Ian O. laser; (1999). Countering The New Terrorism, (ed.) Brace Hofan, John Arquilla, David Ronfeldt, Michelle Zanini.
53. Nicholsm, L.G (1997): "Instructor Development Training a Guide for Security Law Enforcement", Boston M.A Butterworth Heinemann
54. Ogundipe, T. O. and Akinade, A. (2012). Managing Emergency to Terrorism, Human Crises and Drug Abuse for safety. Institute of Security Nigeria.
55. Oliver, A. F. (1965). "Curriculum Improvement; a Guide to Problems, Principle and Procedures Newton Dodd. Mead abd co. in Onwuka. U. (1981).
56. Onashile Y. (2008). Scientific Criminal Investigation, Detection and Prosecution. Institute of Security Nigeria.
57. Paster, J. (2006). Terrorism and Public Safety Policing Cd Rom 90 min.

58. Protection Officer Training Manual 6th Edition, "International Foundations for Protection Officer" Saudi J. Davies and Ronald R. Minion (ed): "Security Supervision Theory and Practice of Asset Protection" 2nd Edition.
59. Robinson D.G and Robinson J.C "Performance Consulting Moving Beyond Training Sib Francisco Bennett Koehler Publisher.
60. Rome, T. L. (2009). "How to Assess the Safety and Security of your Urban centres". www.trialewwirrowe.com
61. Woolcut, L. A. and Rose C. A. (1979). "Business Administration. London Holton Education Publication Ltd.
62. Yomi Onashile (2008). Scientific Criminal Investigation, Detection and Prosecution" Institute of security Nigeria.

UNDERSTANDING COMMUNITY POLICING AND LAW ENFORCEMENT: INTEGRATING SCIENTIFIC-TECHNOLOGY DRIVEN PERSPECTIVES

Barrister Adebayo Akinade, dfisn &
ACP (Rtd) James Olusola Oyewunmi fisn

ABSTRACT

The purpose of the paper is to explore in broad terms how policing and law enforcement need to be developed in communities today.

The community policing is a concept that is fast gaining ground especially among the police and citizens. Its model emphasizes proactive rather than reactive policing. It is also principled on partnership and decentralisation of powers for effective crime fighting.

However, as community policing begins to gain acceptance by the police and citizens, it will reduce crime rate because the public will assist the police in crime fighting by becoming the eye of the police in the community.

Much of the burden of crime control must be borne at the local community level. Enforcement of the law must be strengthened, more and more where crime is spawned in local communities. This objective, for too often, is over looked. However, in any community, it can be achieved by far-sighted police administrations on an enlightened citizens working together for the common goal through the strategy of community policing within the perspectives.

Law enforcement and the administration of justice have been imposed by the utilization of modern scientific management analysis technology and integrated information systems. There is a national and international trend towards the utilization of science and technology in policing at every level.

The paper has implications for how policing organisations and governments develop improved policing strategies in the future.

Modern technology permits community policing to improve and enhance efficiency. There is the need to seek for the ways of how technology can enhance community policing and neighbourhood protection.

This paper will provide insight into technological support for community policing operations. The use of information and communication technology is considered as one of the key elements to significantly improve community policing.

The paper will provide a clear, logical thinking about the role of community policing and law enforcement. It offers a novel concept of public self-policing leading to a new approach to the evaluation of the work of policing organisations. The ideal relationship between police and the public will be carefully examined.

Key terms

Community Policing, Scientific-Technologies, Law Enforcement, Crime Prevention

1.00 INTRODUCTION

Community policing is a concept that is new to the Nigeria police Force. It was not until the early 2000 that the concept started becoming popular in Nigeria. The Nigeria Police Force before the advent of community policing operated on a traditional British semi-military structure of policing that stresses the centralization of powers. This principle of centralization of power is antithesis to the philosophy of community policing that emphasizes decentralization of power. Although, community policing is new in Nigeria, however in the Western world, particularly the United States, the principle has already gained popularity since the late 1970s. Its philosophy emphasizes partnership, proactive policing and decentralization of power. Community Policing stresses that by working together the police and the community can accomplish what neither can accomplish alone. Community policing is a philosophy that emphasizes working proactively with citizens in order to prevent

crime and to solve crime-related problems. Partnership is a key element of Community Policing because the police and the public must partner together in order to adequately fight crime. This will involve the police relinquishing some of their powers to the community so that they can become the eye of the police in the neighborhoods. This can only be achieved if the police earn the trust of the community. However, where there is distrust between the police and the public such a vision becomes unrealistic. Since its introduction, community policing has achieved very little result in Nigeria, especially in the area of partnership between the police and the community due to public distrust of the police and the inability of the police to share some powers with the public. The Nigeria Police who have been used to receiving orders from their superiors find it extremely difficult to share such powers with the community who are very distrustful of police officers. The failure of community policing in Nigeria is also due to the fact that the police are not willing to move away from their traditional policing model which they have been used to for a very long time. This paper therefore examines community policing in Nigeria, its challenges and prospects. It takes a critical look at the history of Nigeria policing, problems of Nigeria police, origin of community policing, philosophy of community police, advent of community policing in Nigeria, as well as the theoretical explanation to Nigeria community policing.

Crime prevention and community policing are enabled and co-evolved with technologies that make the operation possible.

Technology involves designing engineering, materials, components, manufacturing processes, adoption systems integration and diffusion when coupled with science.

Technology can be defined as the application of hard or soft science knowledge, methods and materials to practice arts and skills. **(Akinade, Ogundipe & Adetona 2019)**

Community policing is often described as a philosophy that emphasizes problems solving in partnership with community members to enhance crime prevention methods which may be conceptualized as a social technology.

Security and policing technologies are also physical and range from being relatively simple to complex. Patrolling is one of the basic functions of police personnel in a community environment with patrol equipment which comprises of communication gadgets, maps and compass. **(Akinade A. 2012)**

Law enforcement covers police goals which include the following:

I. The prevention of crime and disorder to peace of communities and societies
II. The protection of life, property and personal liberty for individual security in the community.

Law enforcement officer must at all times perform his duties and he has no right to ignore any violation of the law.

2.00 CONCEPTUAL CLARIFICATION AND PHILOSOPHY OF COMMUNITY POLICING

According to Wrobleski and Hess (2003: 134), Community Policing is an organization- wide philosophy and management approach that promotes community government, and police partnership; proactive problem solving and community engagement to address the causes of crime and other community issues. They also noted that:

"The essence of community policing is to return to the day when safety and security are participatory in nature and everyone assumes responsibility for the general health of the community- not just a select few, not just the local government administration, not just the safety forces, but absolutely everyone in the community" (Ibid. 134).

The philosophy of community policing is for citizens and police to share responsibility for their community's safety. It means that citizens and the police will work collectively to identify problems, propose solutions, implement action and evaluate the results in the community. The idea of Community

policing is quite different from traditional policing that emphasizes strict police authority on crime prevention. In community policing, the police must share power with residents of a community, and critical decisions need to be made at the community level, rather than at police stations (Bohm and Halen, 2005: 215). The goal of community policing is to decentralize police decision making authority. To achieve this goal, it requires the successful implementation of three essential and complementary components or operational strategies namely community partnership, problem solving, and change management (Ibid, 2005: 215). Community policing was intended to address the causes of crime and reduce the fear of crime in affected communities. It employs creative management styles so as to engage responsible members of the public in proactive problem-solving tactics to minimize the level of criminal activities and facilitate law enforcement in the communities. The core elements of community policing are as follows:

- A broader definition of police work;
- A reordering of police priorities giving greater attention to crime and disorder;
- A focus on problem-solving and prevention, rather than incident driven policing;
- A recognition that the „community", however defined, plays a critical role in solving neighborhood problems, and
- A recognition that police organization must be restructured and reorganized to be responsive to the demands of this new approach and to encourage a new pattern of behavior;
- A recognition that police services, operation and management must be decentralized for effectiveness, so that local police officers can speedily address problems and needs encountered at the local levels;
- That the training of police officers must cover the areas of social interactions and problem-solving in addition to traditional policing skills;
- There must be a partnership between the police and the communities in defining or identifying, local problems and needs and developing solutions to identified problems;
- Commitment to development of long-term and proactive policies and programmes to prevent crime and disorder (Law and Justice in Emerging Democracies 2006:13)

Community Policing

There are numerous definitions of community policing but they appear to have three common features: police-community partnerships, a problem-solving approach, and organisational decentralisation (see Oliver, 1998, pp 32-43; see also Community Policing Consortium, 1994). Oliver's (1998, p 51) definition seems most comprehensive:

A systematic approach to policing with the paradigm of instilling and fostering a sense of community, within a geographical neighborhood, to improve the quality of life. It achieves this through the decentralization of the police and the implementation of a synthesis of three key components: (1) ... the redistribution of traditional police resources; (2) ... the interaction of police and all community members to reduce crime and the fear of crime through indigenous proactive programs; and (3) ... a concerted effort to tackle the causes of crime problems rather than to put band-aids on the symptoms.

To this should be added the argument that policing is a concern not just for the police in interaction with communities but also for other agencies with responsibilities for preventing and reducing crime — what Jones and Newburn (2002) have called secondary agencies of crime control.

Considering Oliver's definition, it seems clear that the key feature of community policing is interaction between policing organisations and communities. The other two features are secondary, in that the purpose of the decentralisation is to achieve more effective interaction, and the interaction itself includes forms of joint problem-solving. What is less clear, however, is the nature of the interaction that is envisaged, and how policing

organisations are supposed to instill and foster a sense of community is not made clear at all.

3.00 COMMUNITY POLICING AS STREET-LEVEL BUREAUCRACY

For community policing to work, there needs to be a better balance of the multiple accountabilities of community policing agents. The current situation is described by Brogden and Nijhar (2005, p 57) as follows:

Police agencies define the parameters of what matters are relevant to community accountability and have the means to enforce their determination of the limits of that community influence. In doing so, community policing provides a chimera of accountability. It may legitimate police determination of community goals and priorities, bypassing conventional democratic channels with a more direct interactional relationship rather than opening up new avenues and opportunities for democratic accountability (Klockars, 1988).

This section argues that community police agents are an example of street-level bureaucrats and considers how the literature on street-level bureaucracy can be used to clarify how community policing should be organised.

Street-level bureaucrats were originally characterized by Lipsky (1980) as workers who have high degrees of discretion (or freedom of action) in the organisation of their work, which involves the discharge of public duties and powers including the delivery of services, the dispensation of benefits and the allocation of public sanctions. Street-level bureaucrats see themselves as professionals, who can be trusted to have the necessary expertise to do their jobs, which they define more in terms of relationships than rules. Their relationships with the public, however, are typically asymmetrical because they have specific resources available that the public does not.

Street-level bureaucrats can be held to account in three different directions: vertically upwards, through political or administrative hierarchies, based on legal authority and implemented through task-oriented enforcement or indicator-oriented performance; horizontally, through forms of peer review and collective self-regulation, based on expertise and implemented through professionalized networks; and vertically `downwards', through forms of participatory citizenship, based on democratic values and implemented through impact-oriented co-production. Hupe and Hill (2007) argue that street-level bureaucrats practice multiple accountabilities and the form that accountability takes varies according to four factors: the core issue; the character of the relationships between accountors and accountees; the role of the citizen; and the type of 'accountability regime' (based on the modes of implementation mentioned above) (Hupe and Hill, 2007, p 292).

Applying these ideas to policing practice, core issues can be identified such as the detection or prevention of crime, the enforcement of public order, responsiveness to public demands or the assurance of community safety. Each issue involves different balances of accountabilities, with emphases on different kinds of enforcement, performance and co-production. Each approach to policing gives priority to a particular direction of accountability: traditional law enforcement stresses accountability upwards, problem-oriented policing favours the expertise and judgment of one's fellow officers, while community policing emphasizes co-production between police and community.

For Hupe and Hill (2007, p 294), co-production involves individual compliance with internalized professional standards, organisational conformity to shared goals, relationships of trust between accountors and accountees, and citizen voice in holding to account. In the case of community policing, this means that individual policing agents have to be allowed to develop their own ways of working in partnership with community members, that their organisations have to work with communities to agree on common aims and objectives for community policing, that communities and police have to learn to trust each other, and that all citizens need to be included in police community forums.

The implications of this analysis are profound. It appears that, for co-production of social order to work, at least three conditions must be satisfied. First, each public or set of publics has to operate as a self-organised system, in which order is maintained through the spontaneous interaction between members of the public; second, each policing organisation or set of policing organisations has to function as a separate self-regulating system, in which the rules are defined by the police as street-level bureaucrats acting individually and collectively; and third, self-organised or self-regulating systems of publics on the one hand and policing organisations on the other have to be structurally coupled so that each couple (for example, a public and a policing organisation) itself forms a co-ordination system.

To illustrate this, consider what must happen in a neighbourhood where crime is high but trust in the police is low. The community is likely to be divided so that self-policing is relatively ineffective. Policing organisations are also likely to be ineffective, not least because the community's distrust of them renders them unable to gather the intelligence needed to maintain order in the area. In this situation, police reform on its own cannot be adequate to solve the problem. What must happen simultaneously are processes that raise the quality of the community's self-policing and processes that transform policing organisations into networks of self-regulating teams. The prospects for such a development depend crucially on strategic political decisions about the development and resourcing of such communities.

Processes that improve self-policing can be broadly characterized as involving activities of community development in a wide sense. This includes building forms of human and social capital, collective efficacy, resilience, capacity, self-help, etc. These processes all involve the building and strengthening of co-operative interaction. For the maintenance of social order, key styles of such interaction are civility and sociability (Misztal, 2000). The relationship between such styles and high-crime, low-trust communities, however, is complex and little understood. It is possible, for example, that levels of civility and sociability might actually be quite high in such communities — notorious gangsters might act quite civilly to one another and sociability can be very strong not only within a criminal gang but also between gang members and their local community — while at the same time members of different gangs are shooting and murdering one another. In this case, `low trust' characterizes the relationship between community members and policing organisations, and between gangs, but not relationships within certain sections of the community (gangs, tribes, elites, in-groups, cliques, etc.), At the other extreme, it is possible that levels of civility and sociability might be very low in a low-crime, high-trust community, where people 'keep themselves to themselves' but are very trusting of policing organisations.

Consequently, each community has to be assessed individually in order for it to be possible to select appropriate plans of community development action — that is, to decide whether to focus more on improving civility and sociability (e.g. with an emphasis on things like garbage, feces, noise, public drinking and forming community groups) or on correcting forms of 'false' civility and sociability such as those associated with organised criminal activity and structural inequality (see Somerville, 2009). A significant complicating factor here is that undertaking such assessments and planning requires participation by appropriate individuals and organisations (not only policing organisations) from outside the community. A variety of expertise, for example, is required for such an under-taking — in such fields as economic development, housing, healthcare, family support, social regeneration, neighbourhood management and planning, open space and recreational management, transport planning and management, etc.

4.00 PUBLIC SELF-POLICING AND COMMUNITY POLICING

The term 'informal social control' is commonly used to refer to the maintenance of order by members of the public or of a particular

community. Silver and Miller (2004, p.553), for example, define it as the 'willingness of neighborhood residents to actively engage in behaviors aimed at preventing criminal and deviant behavior in the local area'. Such activity, however, is not necessarily informal, nor is it appropriately characterised as 'social control' she advocated the mixed use of public space, in order to maximise the number of eyes and ears of the public engaged in this practice. The explanation for her findings could be that potential transgressors are deterred by the risk, however slight, that others might intervene or might bear witness against them later on, or perhaps by the shame that might be attached to being seen as a transgressor. This would mean that the effectiveness of such action by others depends upon the response to it in terms of individual self-policing, whether 'self here is understood in terms of a rational self (calculating the balance of risk and reward) or in terms of an ethical self (concerned with protecting and enhancing one's sense of self-value or self-esteem, as well as the esteem with which one is held by others).

Later, Jacobs' insight was 'explained' in a different way, in terms of what is called `routine activities theory' (Cohen and Felson, 1979; Felson, 1998). According to this theory, crime (and, by extension, other forms of transgression) is largely the result of three factors coming together: a likely transgressor, a suitable target (or victim) and the absence of effective intermediaries either to 'handle' the transgressor or to 'guard' the target or victim. In Jacobs' scenarios, members of the public act mainly as guardians of the public space (which includes all kinds of potential targets and victims), though they may also at times intervene in order to 'handle' potential or actual transgressors (e.g. challenging strangers, and 'have-a-go' heroes). This approach therefore highlights the importance to social order of having effective intermediaries.

But what makes for effective intermediaries? Understandably, people are prepared to challenge strangers, step forward as witnesses, and so on, only where they feel confident of their own safety and a reasonable level of trust in criminal justice institutions. Effective intermediation requires: 'trusting others in the sure knowledge that they won't be let down or disillusioned' (Shaftoe, 2004, p 201). 'Informal social control' therefore depends crucially on trust, which can be understood in Luhmann's (1986) terms as the willingness to assume risk.

Mutual monitoring and a willingness to intervene founded on confidence and trust are therefore key ingredients of 'informal social control'. Strictly speaking, however, as Misztal (2000) has shown, such processes are not purely informal because they involve a balance between formality and informality, specifically between the informality of mutual monitoring and surveillance and the formality of codes of behaviour embedded in public and institutional cultures. Nor does it seem appropriate to describe such processes as involving 'social control', insofar as the latter appears to imply that certain individuals or a group of them (namely, the so-called law-abiding') are controlling other individuals or groups (namely, 'deviants' of some kind), whereas here it is a case of everyone controlling everyone else. For these reasons, it may be better to call this 'self-governance' (Kooiman, 2003, p 83) or self-regulation. Self-policing can then be understood as a type or aspect of self-governance or self-regulation.

"But what is the 'self' here? What is the public that is policing itself? Harris (2006, p 63) shows that readiness to intervene when a rule is breached is related to many different factors, including whether the perpetrators of the breach are known to the witness or whether the witness is known to them; whether it occurs in the witness's own immediate neighbourhood (Harris, 2006, p 64); whether fellow bystanders are seen as people like them (Levine et al., 2002, p 3); whether the authorities are perceived as responsive, effective, supportive or trustworthy (Silver and Miller, 2004, p 558); the perceived risk of harm to themselves; and the perception of one's own responsibility/duty or of the value of intervening (Hawdon et al., 2003; Barnes and Baylis, 2004, p 101).

5.00 SCIENTIFIC AND TECHNOLOGICAL APPROACHES IN COMMUNITY POLICING AND LAW ENFORCEMENT

Security operation can be defined as all activities, procedure, action taken or involved in the protection of life and property and provision of a peaceful and stable environment for the daily conduct of lawful activities by individuals and groups within the community. Even though security operations are mere human activities guided by social relations, be it offensive or defensive, they are more effectively consummated with the application of scientific knowledge to the acts and of course the use of tools, equipment and electronic gadgets whose functions are science based. Most tools and equipment use security operation and sometimes security procedures itself are products and applications of scientific knowledge. Technology and science have increased reliance on the use of machine for observation and recording in security operations. **(Akinade A. & Aderibigbe A. 2018)**

Security Equipment and Tools

The computer as an equipment is used for keeping and updating security records. Microfiche microfilming replaced cumbersome paper work and are used for reducing records into smaller size for easy and compact storage. Other tools and equipment include tape recorders, Closed Circuit TV, camouflage cameras, lock picks, microphones, transmitters, transmitter detector, explosive detectors, metal detectors, x-ray, letter-spray, portable video cassette recorder, letter-bomb detector, bomb blanket, bulletproof vest, frequency jammers, telephone analyzers, walkie-talkie, night vision equipment, spectacle for rear surveillance, spectacle for agent identification, attack light, attack baton, direction finders used for surveillance, technical surveillance car van, bugging devices, alarm system, cassette erasers, voice stress analyzer, lie detector.

One example of procedures in security operation that are laden with scientific knowledge is forensic investigation of finger printing, questioned documents and analysis of writing, drug/blood `saliva Semen analysis, photography traces.

Another very essential tool or procedure in security operations are map and map reading. A map is a representation of any portion of land drawn to scale on paper. Topographical map is the most important for security operations because it contains all the necessary details for an operation e.g. mountains, deserts, forests, lakes, rivers, valley, etc. Others are political map, geological map, atlas maps, etc.

The usefulness of map in security operation is enormous:

- It helps the commander to know the right choice of route for the operation;
- Identify your own location, positions and that of the enemy;
- Analyse, appreciate, and make use of the physical features on the ground e.g. rocks, river Measures time and distance.
- It helps to know beforehand a likely dangerous place and how to avoid it before the D-day.
- For quick terrain analysis in order to ease movement in the areas of operation.

Map reading on other hand deploys the knowledge of contour, conventional signs in geography, fraction, decimal, gradients and trigonometry in mathematics especially for plotting bearings on map. It is necessary to conclude by mentioning that every security organisation has its own technical directorate which is purely made up of scientists carrying out scientific activities. **(Akinade A. & Aderibigbe (2018)**

Technological Advancement

Technology has been defined as the use of mechanical arts and applied sciences. It refers to inventions, including tools, devices, techniques and processes that people make, use to survive and prosper. Technology has made it much easier for people to satisfy their needs and desires.

In the last two decades, technology has opened new doors and created new pitfalls for both criminals and law enforcement.

Advancement in communication and technology has dramatically expanded legitimate commercial enterprise between states, thereby shrinking distance rendering state frontiers porous, and opening up previously unimaginable opportunities for commercial, political and social interaction.

Technology is a fact of life in both the legitimate and the criminal world and there is no question that organised crime group use computers. wireless phones and the internet to communicate and to do business.

Of concern is the scope and sophistication of their use of technology and their knowledge of law enforcement interception; surveillance and other capabilities.

Television, radio, microwave and landline communications technique have improved and make security work more effectively and efficiently.

Surveillance communicating device have become more sophisticated and more versatile. Satellite communication devices are being enlisted in the anti-crime effort.

Fingerprint, mug shots, criminal histories and reports may be canned, translated back to graphic form without the necessity of moving the original material over a long distance.

Methods are now being developed which will greatly increase the speed of transmission. The science and technology of optics will be increasingly associated with computer system in security environment.

In criminalistics techniques, computerized methods of' classifying, identifying, comparing and analyzing physical evidence are being developed along with medium and long-range research. Computer science and technology will provide ultimately for more reliable valid, standardized and consistent methods for statistical research in the administration of criminal justice.

The transfer of data may be by courier, telephone, teletype, mail, facsimile transmission, microwave, radio or television. Transmission security uses devices to prevent electronic eavesdropping such as scramblers, coded messages, key receivers shielding as well as methods of identification of senders and receivers, access control over Information devices, classification burning and shredding waste paper and security or storage methods. **(Akinade A., Ogundipe T.O & Adetona S.O 2019)**

6.00 APPLICATION OF TECHNOLOGY TO PRACTICE OF COMMUNITY POLICING

It is important to examine different aspects of ethics and unethical behaviour for law enforcement and police officers at all levels in reference to the use of technology. Technology has enabled law enforcement to respond more quickly to calls for service, use more advanced nonlethal compliance tools, and use the Internet to combat crime. The foundation of ethical practices is based on the fundamental human right of the Constitution supplemented by the courts of the Nigeria States delivering decisions that affect the use of technology by law enforcement officers and administrators. Using these guidelines, officers are expected to complete their daily duty assignments with the use of technology both legally and ethically. An officer's ethical foundation and training allow them to exercise discretion in the enforcement of laws, sometimes blurring the line between what is ethical and legal.

Law enforcement application of technology increases the capability of policing throughout tile world. Technology has played a progressing role in the way security personnel perform their daily duties. Among the tools commonly used by the law enforcement officers are the semi-automatic pistol a collapsible baton, Oleoresin Capsicum, spray and the taser. Ocspray can deliver a blast of chemicals to tile eyes of' a suspect leaving them disoriented and usually full of complaint. The taser is a weapon that delivers 50,000 volts to its target, completely immobilizing the subject until they can be brought under control. These tools ire non-lethal and used at various levels of compliance.

The operation of criminals and terrorists are indiscriminate Hence, tracking them requires careful planning, preparation and cooperation among Security operatives and foreign Countries. Since terrorists and criminals have sinister motives, they often hide their identities or use falsified identities. In order to forestall criminal and terrorist's attacks, intelligence and warning systems are put in place for detecting and preventing future attacks. The framework for tracking criminals using imaged-based, height, posture and body detection techniques. **(Akinade A & Aderibigbe A. (2018)**

Criminal detection could be very difficult and challenging task for security agencies especially in a situation where the criminal is showing chameleon-action in posture. The criminal may use mask or other forms of disguise. Hence, face-recognition and finger print may be effective in detecting him/her.

7.00 PATTERNS OF CRIMINAL IDENTITY AND PERSONAL DATA IN INTELLIGENCE GATHERING IN COMMUNITY POLICING

There is the need to ensure that resources being committed to new technologies that are aimed at tracking criminals do not go down the drain. Also, any technology being introduced to track criminals does not generate false positives that would subject innocent persons to unnecessary scrutiny that could impinge on their rights and freedom. Although, there are many tools and techniques use for crime detection. Existing systems that perform person's identification and tracking have several advantages, but also have drawbacks. For instance, Roger Clarke (2004), reports that people's hands do not differ enough for {hand geometry} to be used as an identification system. The Economist (2003) posits that "*around 5% of people do not have fingerprint*" **Leyden (2002)** reports that comprehensive tests of 11 consumer-oriented biometric products showed that the devices were more of the nature of toys than of serious security measures" and that large scale application of' iris technology (by the UNCHR in Afghanistan) has not been used to generate measures of reliability and quality.

Facial recognition is one of the soft -biometric means of tracking criminals, yet it has some drawbacks like eye colour which are easily influenced by light situation. Also, in the use of facial recognition it has been found that there could be a situation where a short person is having a tall face and vice-versa. Hence, it may not be used to judge accurately.

Height has been long used in forensic measures to detect possible suspects, it is however, not distinctive enough to be used in biometric identification. Hence, estimating the heights of the tracked subjects using any camera and assuming any distance in capturing could provide us with an important additional feature, thereby making the object tracking over different scenes more robust. For instance, **(Ben Abdelkader et al., 2002)** developed C1 parametric method to automatically Identify people in low - resolution video by estimating the height and stride parameters.

There is the need to focus on uncovering patterns of' criminal identity deception based on actual criminal records and suggest an algorithmic approach to revealing deceptive identities.

It is a common practice for criminals to lie about their personal data. Hence, the ability to validate identity can be used as a warning mechanism and the deception signals the intent to commit future offenses. Terrorists do not act alone but rather they operate in a network. They may be linked together through various social, ideological, religious and communication networks. This network may be complex to unravel. Hence, there is the need to properly understand the way relationships are formed or communication is maintained within or between terrorist groups. The link structure of' the web represents a considerable amount of' latent human annotation **(Gibson, 1998).** Thus, by analyzing and visualizing hyperlink structures between terrorist-generated web sites and their contents, we could discover the structure and organisation of terrorist group networks, capture network dynamics, and understand their emerging activities. So, an intelligent web

portal, called Dark Web Portal, to help terrorism researchers collect, access, analyse, and understand terrorist groups was developed (Then **and Reid, 2004).**

Height detection of objects can be used both for soft-biometrics and as an object tracking feature. Unwanted area is eliminated and the focus object is extracted to determine the identification features **(Jeges and Mate, 2006)** and use it to search for similar subject in a smaller set of possible candidates. For object tracking, it can be used for temporal and spatial correspondence analysis as well or simultaneously for both in case of disjoint cameras **(Madden and Piccardi, 2005).**

Gait based identification also strives for extracting human height. The exploitation of gait can be seen in **(Lv et al., 2002**), where in the camera used is a calibrated one using a walking person. Sonic other interesting methods of human height estimations can be found in the literature, like the one in **(Bernardin et al., 2006),** where the acoustic source localization of the speaking person is used for this purpose.

Also, anonymous motion sensors were used in rooms and switch sensors on daily-use objects, and resident activity models to identify and track their activities and locations. They propose using a particle filter that uses Markov state transition and sensor use models learned from short term training data, obtained using a tag and track approach or manual labelling. The main advantage of this approach is that the simple single-pixel sensors are cheap and easy to install, and are not perceived to be invasive or inconvenient. However, an important drawback of this approach is low accuracy: this system was reported to have 70% accuracy when 3 residents over a week-long period are used. These accuracy rates may be level-headed for some applications, but mystifying the identities of residents more than a third of the time could cause problems in the case of medical monitoring **(Wilson and Atkeson, 2005).**

8.00 LAW ENFORCEMENT AND POLICING: Principles of Standards Functions

In order to make the law effective, it must be enforced. While it is true that the ruthless enforcement of the law can be tyrannical, it is also just as true that apathetic or indifferent enforcement of the law can make the law sterile and meaningless.

Law enforcement covers the following concepts and terms, "**police authority**", "**police power**", **police goals**", **police methods**", and "**police role**". Although they are often used interchangeably.

Police Authority means the right of the state to act relative to the general security, safety and welfare.

Police Power means the force which is utilized by the state in acting relative to the general health, safety, and welfare.

Police Goals refer to two major objectives:

1. The prevention of crime and disorder and the preservation of the peace (for community security).
2. The protection of life and property and personal liberty (for individual security).

Police goals are described as "protecting lives and property and keeping the peace". The professional police of today realizes the importance of preventing crimes and disorder and his genuine duty to secure personal liberty for all citizens. (Danbazau A.B & Husain S. 1990).

These goals are achieved by five major methods:

1. **Crime Prevention**--by working with the juveniles; by cooperating with probation and parole personnel; by educating the public; and by providing visible evidence of police ability and availability.

2. **Crime Repression**--by investigating crime; by identifying and apprehending offenders; by recovering stolen property and by assisting in the persecution and conviction of those who violate the law. Most working policemen would have

regarded this method as the entirety of the police task. As the officer as increase his perspective, he has come to see himself as a part of criminal justice, working with prosecutors, courts, probation, correctional, and parole personnel, and has enlarged his methods and emphasis. He now regard crime regression as necessary and proper, but not the sole reason for his existence; he also accepts crime prevention and protection of personal liberty as equally necessary and proper methods to achieve his goals.)

3. **Regulation of Noncriminal Conduct**--by controlling the noncriminal citizen in such areas as traffic (Vehicles, parking, pedestrians), public events (crowd control), and social relations (domestic disputes), in order to maintain community tranquility.

4. **Provision of Services**--by rendering information, directions, advise, and general assistance, by counselling and referral, and through special services such as licensing and registration.

5. **Protection of Personal Liberty** by protecting the individual citizen against unwarranted interference on the part of the state; and by instructing the citizenry in terms of their duties, obligations, right, and privileges in reference to the law.

Standard Police Functions

The standard police functions are stated below: -

a) Police, as an agency of the criminal justice system, have a major responsibility for dealing with serious crimes, efforts should continually be made to improve the capacity of police to discharge this responsibility effectively. It should also be recognized, however, that police effectiveness in dealing with crimes is often largely dependent upon the effectiveness of other agencies both within and outside the criminal justice system. Those in the system must work together through liaison, cooperation, and constructive joint effort. This effort is vital to the effective operation of the police and the entire criminal justice system.

b) To achieve optimum police effectiveness, the police should be recognized as having complex and multiple tasks to perform in addition to identifying and apprehending persons committing serious criminal offenses. Such other tasks include protection of certain rights such as to speak and to assemble, participation either directly or in conjunction with other public and social agencies in the prevention of criminal and delinquent behavior, maintenance of order and control of pedestrian and vehicular traffic, resolution of conflict, and assistance to citizens in need of help such as the person who is mentally ill, the chronic alcoholic, or the drug addict.

c) These standards are based on the view that this diversity of responsibilities is likely to continue and, more importantly, that police authority and skills are needed to handle appropriately a wide variety of community problems.

Scope of Standards

To ensure that the police are responsive to all the special needs for police services in a democratic society, it is necessary to:

I. Identify clearly the principal objectives and responsibilities of police and establish priorities between the several and sometimes conflicting objectives;
II. Provide for adequate methods and confer sufficient authority to discharge the responsibility given them;
III. Provide adequate mechanisms and incentives to ensure that attention is given to the development of law enforcement policies to guide the exercise of administrative discretion by police.
IV. Ensure proper use of police authority;
V. Develop an appropriate professional role for and constraints upon individual

police officers in policy-making and political activity;
VI. Provide police departments with human and other resources necessary for effective performance;
VII. Improve the criminal justice, juvenile justice, mental health, public health system of which the police are an important part;
VIII. Gain the understanding and support of the community; and
IX. Provide adequate means for continually evaluating the effectiveness of police services.

Police Objectives and Priorities.

Factors accounting for police responsibilities are very vital to the society.

The wide range of government tasks currently assigned to police has been given, to a great degree, without any coherent planning by state or local governments of what is overriding objectives or priorities of the police should be. Instead, what police should do is determined largely on an ad hoc basis by a number of factors which influence their involvement in responding to various government or community needs. These factors include:

I. broad legislative mandates to the police;
II. the authority of the police to use force lawfully;
III. the investigative ability of the police;
IV. the twenty-four availabilities of the police; and
V. community pressures on the police.

In assessing appropriate objectives and priorities for police service, local communities should initially recognize that most police agencies are currently given responsibility, by design or default:

I. to identify criminal offenders and criminal activity and, where appropriate, to apprehend offenders and participate in subsequent court proceedings;
II. to reduce the opportunities for the commission of some crimes through preventive patrol and other measures;
III. to aid individuals who are in danger of physical harm;
IV. to protect constitutional guarantee;
V. to facilitate the movement of people and vehicles;
VI. to assist those who cannot care for themselves;
VII. to resolve conflict;
VIII. to identify problem that are potentially serious law enforcement or governmental problems;
IX. to create and maintain a feeling of security in the community;
X. to promote and preserve civil order; and
XI. to provide other services on an emergency basis.

9.00 POLICING AND LAW ENFORCEMENT UNDER THE 1999 CONSTITUTION

Under the 1963 constitution the constitution permitted the establishment of LOCAL POLICE on a provincial basis, this had made it possible for the northern and western regional governments under the constitution to retain and expand the local police forces established and maintained by some of their nature authorities under the nation's ordinance of 1943, this is evidenced in section 105 (7) 1963 constitution.

The 1999 constitutions provides that there shall be established Police Force. It prohibits the establishment for the federation or any part thereof any other police force and vests the legislative competence to make laws for the organization and administration of the police exclusively in the National Assembly which is empowered to make provisions for the establishment of branches of the Nigeria Police Force (Section 214 Constitution of the Federal Republic of Nigeria, 1999.

Plural, State and Community Based Policing

Before examining the need for establishment of state policing and community policing in Nigeria, it is important to underscore the state of policing in Nigeria vis a vis the performance of the police in the protection of lives and properties with police Act cap P.19 LFN 2004.

There is a general perception that the existence of a country of 140 million people belonging to various ethics groups with distinctive population, language, land mass,

religion and cultural attitudes. It has been argued that the genesis of the inability of the Nigerian police to effectively carry out their duty is traceable to the introduction of a single police force for the whole country as opened by the late governor Ambrose Alli of Old Bendel State in Sunday times of October 18, 1981 pg.18.

It is argued that only a plural or state police can provide a most conducive platform for the implementation of community policing. Community policing stresses policing with and for the community rather than policing of the community. It aspires to improve the quality of life in communities. In improving the quality of life, it aims to solve community problems alongside the community and as defined by the community.

The amendment of the constitution to establish state police will create a platform for the people in the local communities to identify with the police as "their police" as suggested by B.O. Nwabueze in his book "federalism in Nigeria under presidential constitutions London Sweet & Maxwell pg 123 & 124-1983. The call for the amendment of the constitution to provide for the establishment of a plural or state police needs to be appraised in the light of possibility of abuse of the use of police as an instrument of oppression.

One of the options available to achieve effective reform of the present Mono Police Force, is decentralization whereby the different six geopolitical zones would be allowed to establish regional police in which the states composing the zone will collectively fund and exercise operational and commend control over their regional police force. These zones are North West, North East, North Central, South West, South East and South South. Another option is to allow for the establishment of state police in each state of the federation. The third option is to allow for birth regional and police forces to be established.

Obviously, the adoption of any of the proposed options will necessitating the amendment of the relevant of the relevant provisions of the constitutions to provide for the establishment of Federal, Regional, State and Local Police System.

The Regional Police or State Police will be empowered to enforce Laws and Regulation of the States within the Region or the State. The Federal Police will be responsible for enforcing federal laws and regulations. Within this framework Local Government Police can also be established to operate in the local communities to enforce Local Government Bye-Laws and contribute towards law enforcement and intelligence gathering in the Local Communities.

It has been suggested that the National Assembly should amend the Police Act. Capp 19LFN 2004 to provide a platform for state involvement in policing.

10.00 COMMUNITY POLICING AND POLICE ACT, 2020

The Nigeria Police Act, 2020 part XIV on community policing committee was enacted to ensure smooth operation of community policing in Nigeria.

Section 113 stipulated the Establishment of Community Policing Committee which states thus:

1) "For the effective and efficient policing of communities in a State or Federal Capital Territory, the commission of police of a state shall established community police committee and shall consist of representatives of the police force and the local community in the state"
2) "A commissioner of police shall establish community sub-policing committee at all Divisional Police Headquarters in the State or Federal Capital Territory
3) "Subject to section 116 (1) (b) of this Act, the Commissioner of Police and members designated by him from time to time for the purpose, shall be members of the Policing Committees and Sub-Policing Committees established at various police formations".

Section 114 stipulated the Establishment of Community Policing Committee which states Thus:

1) "A Commissioner of Police of a State or Federal Capital Territory shall, in collaboration with the relevant stakeholders in the community, establish Divisional Community Policing Committee (in this Act referred to as "Divisional Policing Committee"
2) "A Divisional Policing Committee shall, in collaboration with the relevant stakeholders in the community, establish Divisional Community Policing Sub-Committee in all police formations in the Division".
3) "Subject to section 116 (1) (b) of this Act, the Divisional Police Officer and the members designated by him, from time to time for that purpose, shall be members of the Divisional Policing Committee concerned".

Section 115 stipulated the Establishment of State Community Committee which states Thus:

1) "A Commissioner of Police of a State shall, in collaboration with the State Executive Council, establish a State Community Police Committee".
2) "A State Community Police Committee shall, subject to subsection (3) of this section, consist of representatives of Divisional Community Police Committees designated for that purpose by the Divisional Community Police Committees of a State concerned".
3) "Subject to section 116 (1) (b) of this Act, Commissioner of Police in a State and the members designated by him, from time to time for the purpose, shall be members ofthe State Community Police Committee concerned".

Section 116 stipulated the Objectives of Community Policing Committees which states Thus:

1) The objectives of the Committees are to:

a) Maintain a partnership between the community and the Police Force;
b) Promote communication between the Police Force and the community;
c) Promote co-operation between the Police and the community in fulfilling the needs of the community regarding policing;
d) Improve the police service to the community; and
e) improve transparency and accountability in the provision of police Services to the community.

2) This section does not prevent police liaison with the community by means other than Policing Committee, Sub-Policing Committee and Divisional Policing Committee.

Section 117 stipulated the Duties of Community Policing Officers which states Thus:

1) The duties of Community Policing Officers shall include assisting the Police in:

a) Crime detection and protection;
b) Conflict resolution.
c) Criminal intelligence gathering and dissemination to the local Police Commanders;
d) Maintenance of Law and Order;
e) Deployment to complement the conventional Police in the patrol of the public space within their local communities;
f) Reassuring and advising the public-on-public safety, crime prevention and security tips;
g) Dealing with minor offences and social vices;
h) Working with the community, schools, and young people, business communities, religious bodies, cultural groups, community-based Associations, recreational centers and hospitality businesses toward crime control; and
i) traffic management and school safety duties.

2) The Inspector-General of Police in implementing Community Policing shall promote organizational strategies that support the systematic use of partnerships and problem - solving techniques to proactively address conditions that cause crime, social disorder and fear of crime.

3) The Inspector-General of Police in implementing Community Policing may vary strategies according to the needs of the communities involved and the cultural context. Local models will vary and evolve according to the differing needs of differing communities, whilst retaining and sharing the same set of goals and basic principles.

Section 118 stipulated the Functions of Community Policing Committee which states Thus:

1) A State Community Policing Committee or Divisional Community Policing
2) Sub-committee shall perform the functions it deems necessary and appropriate to achieve the objects stated in section 116 of this Act.

Section 118 stipulated the Procedural matters which states Thus:

1) A Committee, Sub-Committee and Divisional Committee shall:

a) Elect, from amongst its members, a chairman, Vice-Chairman and a Secretary who shall be police officers;
b) Determine the number of members to be assigned by the State Commissioner or Divisional Police Officer to serve as members of the Committee or Sub-Committee concerned;
c) Determine its own procedure and cause minutes to be kept of its proceedings; and
d) Whenever it considers necessary, co-opt other members, experts or community leaders to the Committee, Sub-Committee and Divisional Committee in an advisory capacity.

2) Members of the Committee, Sub-Committee and Divisional Committee shall render their services on a voluntary basis and shall have no claim to any remuneration solely for services rendered to the Committee, Sub-Committee or Divisional Committee.
3) The majority of the members of a Committee, Sub-Committee or Divisional Committee shall constitute a quorum at any of its meetings.
4) In the absence of the Chairman of a Committee, Sub-Committee or a Divisional Committee at a meeting, the Vice Chairman shall preside over the meeting, and if both the Chairman and Vice-Chairman are absent, the members present shall elect one of them present to preside over the meeting.

11.00 MEASUREMENT OF EFFECTIVENESS OF COMMUNITY POLICING: Science and Technology Perspectives

The effectiveness of the community policing should be measured generally in accordance with the ability of the police force to achieve the objectives and priorities selected for police service in individual communities. In addition, the effectiveness of police should be measured by their adherence to the principles of police practice. This means that, among other things, police effectiveness should be measured in accordance with the extent to which they perform the fellow tasks:

I. safeguard freedom, preserve life and property, protect the constitutional rights of citizens and maintain respect for the rule of law by proper enforcement thereof, and, thereby, preserve democratic processes;
II. develop a reputation for fairness, civility, and integrity that wins the respect of all citizens, including minority or disadvantaged groups;
III. use only the amount of force reasonably necessary in responding to any given situations;
IV. conform to rules of law and administrative rules and procedures, particularly those which specify proper standards of behavior in dealing with citizens
V. resolve individual and group conflict; and
VI. refer those in need to community resources that have the capacity to provide needed assistance.

Traditional criteria such as the number of arrests that are made are inappropriate measures of the quality of performance of individual officers. Instead, police officers should be rewarded, in terms of status,

compensation, and promotion, on the basis of criteria defined in the rules and regulation which directly relate to the objectives, priorities, and essential principles of police service.

A new wave of technology and scientific approach needs to be introduced into practice. The application of science and technology has great social-economic values and social benefits in the area of criminal justice, scientific security and technology approaches which should focus on criminal justice, intelligence and police science. Modern technology and scientific solutions will enhance community policing and security administration, intelligence and surveillance in community policing.

Technology and scientific approach to prevention, monitoring, tracking and exposure of crimes is a collective responsibilities and primary goal of all law enforcement and security agencies. Police personnel should no longer rely on old and traditional experience, especially as technologies and scientific advancement has brought new dimension to various crimes which can only be combated using modern technological and scientific devices. Police and security personnel can use smartphones, two-way radios, panic alarms and automatic alarms during patrol to periodically check security threats and vulnerabilities in the communities. Intelligence and surveillance technologies can document events and collect information and intelligence gathering which are useful for security, police operations, crime detection and prevention. Technological and scientific devices can be used for law enforcement and police operations because they response more quickly to calls for security and police services.

12.00 CONCLUSION

The recommendations made in these standards require particular attention at the level of state and federal government levels. Along with the recommendations relating specifically to police agencies, however, it should be recognized that police effectiveness is also dependent, in the long run, upon:

I. the ability of government to maintain faith in democratic processes as the appropriate and effective means by which to achieve change and to redress individual grievances
II. the willingness of society to devote resources to alleviating the despair of the culturally, socially, and economically deprived; and
III. the improvement of the criminal justice, community policing and public safety system as effective ways of dealing with a wide variety of social and behavioral problems.

Community Policing, understood as policing by an organisation that is distinct from the community yet gives high priority to interaction with the community. The paper therefore went on to evaluate the evidence on community policing, mainly from the perspective of the effect of such policing on the community. This also seems to be unfinished business, as it turns out that community policing remains largely untried, in that high priority is almost never given to the community. In most areas in most countries, whether they be 'close to the community' or not, the police remain a law unto themselves.

The paper then attempted to make sense of this by conceptualizing community policing as a form of street-level bureaucracy. By juggling multiple accountabilities (to their bosses, to the law, to their colleagues and to the public), police officers, like other street-level bureaucrats, are able to turn many potentially unfavourable situations to their advantage. This is not necessarily a bad thing, for example, in a context where there are high levels of trust between the officers and members of a public that is policing itself well. In other contexts, however, it is problematic, being likely to result in neglect and abuse, by both police and public. The last part of the paper, therefore, considered how such problems might be tackled or prevented. The nature of the problems needs to be specified as clearly as possible (again, further work is required here), but it is expected that there will be particular emphasis on forms of community development, encouraging communities to

become more effectively self-policing, together with radical reform of policing organisations to make them capable of structurally coupling with the emergent forms of public self-policing. Needless to say, perhaps, this is not what happens at the moment.

For community policing to have an inroad in Nigeria, the Nigeria police force must have a complete paradigm shift *from* its traditional model of policing to a more community-oriented policing that stresses community partnership, decentralization of powers, and proactive policing. The policing model should be that of partnership with less emphasis on regulatory powers and sanctions with greater reliance upon compromise and cooperation that would serve the public better rather than the traditional model of policing (Iwarimie-Jaja, 2006: 16). More importantly, the police must improve its public image so that they can earn public trust. This can only be achieved when they show a caring attitude towards the public rather than use of brutal force on them and demanding for money before services are delivered. Science and technological approaches in community policing should be encouraged.

REFERENCES

Akinade A. Ogundipe T.O. and Adetona S.O. (2019) "Technologies and Forensic Investigation for Security and Criminal Administration" ISN Publication series, Lagos.

Akinade A. (2012) "Community Policing: Strategic Approaches to Crime Prevention" ISN Publication Series, Lagos

Akinade A. & Aderibigbe A. (2018) "Legal and Ethical Issues in Security Technology and Communication". ISN Publication Series.

Akinade A. (2012) "Law Enforcement and Internal Security: Responses to Security Challenges and Threats" ISN Publication Series, Lagos.

Bohm, R. and K. N. Haley (2005) Introduction to *criminal Justice.* 4th edition. New York: Mc-Graw-Hill.

Ehindero, S. 0. (2006: 12-13) „The Challenge of Law Enforcement in a Federal Nigeria". *A paper presented at the Nigerian Bar Association Annual General Conference (NBA)* on *Law and Justice in Emerging Democracies: The Challenge Before The Legal*

Profession in Africa. Held in Port Harcourt, Rivers State, Nigeria between 26th August and 1St September, 2006.

Haralambos, M. and M. Holborn (2005) Sociology: *Themes and perspective.* 5th edition. London: Harper Collins.

Ibeanu, 0 (2007) "Criminal Justice Reforms: Policing Services Delivery", in *Reforming For*

Justice, ed. Joseph Chu"ma Otteh, Apapa: Access to Justice. Igbo, E. U. M. (1999) *Introduction to Criminology.* Nsukka Afro-Orbis Publications Ltd. Iwarimie-Jaja, (2003) *Criminology: The Study of Crime.* Port Harcourt: SIJ Publishers. Iwarimie-Jaja, D. (2006) "A Democratic Police System For Nigeria". *Nigerian Journal of Criminal Justice Affairs* Vol. 1 January 2006 (pp. 16).

Kupolati, T. (2007) *Remaking the Nigeria Police.* 1st edition. Ilupeju: Renaissance Law Publishers.

Wrobleski, H. M. and K. M. Hess (2003) *Introduction to Law Enforcement and Criminal Justice.*7th Edition. Belmont: Wadsworth/Thomson.

Ballintyne, S. and Fraser, P. (2000) 'It's good to talk but it's not good enough: fictive consultation as a key to safer communities', in S. Ballintyne, K. Pease and V. McLaren (eds) Secure foundations: key issues in crime prevention, crime reduction and community safety, London: Institute for Public Policy Research, pp 164-88.

Barnes, J. and Baylis, G. (2004) Place and parenting: A study of four communities,

London: Institute for the Study of Children, Families and Social Issues, University of London.

Bayley, D. (1994) Police for the future: Studies in crime and public policy, Oxford: Oxford University Press.

Boostrom, R. (2000) Enduring issues in criminology, San Diego, CA: Greenhaven Press.

Bottoms, A. E. and Wiles, P. (2002) 'Environmental criminology', in M.

Maguire, R. Morgan and R. Reiner (eds) The Oxford Handbook of Criminology (3rd edn), Oxford: Oxford University Press, pp 620-56.

Brady, J. P. (1982) Justice and politics in people's China: legal order or continuing revolution? New York: Academic Press.

Brogden, M. and Nijhar, P. (2005) Community policing: National and international models and approaches, Cullompton: Willan Publishing.

Brown, A. (2004) 'Anti-social behaviour, crime control and social control', Howard Journal of Criminal Justice 43, 2: 203-211.

Bursick, R. and Grasmick, H.G. (1993) Neighborhoods and Crime: The Dimensions of Effective Crime Control, Lexington Books, New York, NY.

Chappell, A.T. and Lanza-Kaduce, L. (2004) Integrating sociological research and theory with community-oriented policing: bridging the gap between academics and practice. Available at: www.clas.ufl.edu/users/chappell/Lonn %20paper.pdf.

Cohen, L. and Felson, M. (1979) 'Social change and crime rate trends: a routine activity approach', American Sociological Review vol 44, no 4, pp 588-608.

Community Policing Consortium (1994) Understanding community policing: A framework for action, Washington, DC: Bureau of Justice Assistance, US Department of Justice.

Cordner, G.W. (1998) 'Problem-oriented policing vs. zero tolerance', in T. O'Connor Shelly and A.C. Grant (eds), Problem-oriented policing: Crime-specific patterns, critical issues and making POP work, Washington, DC: Police Executive Research Forum.

Crawford, A. (1997) The local governance of crime: Appeals to community and partnerships, Oxford: Oxford University Press.

Crawford, A. (2003) "Contractual governance" of deviant behaviour', Journal of Law and Society vol 30, no 4, pp 479-505.

Crawford, A. and Lister, S. (2004) The extended policing family: Visible patrols in residential areas, York: Joseph Rowntree Foundation.

Crawford, A., Lister, S., Blackburn, S. and Burnett, J. (2005) Plural policing: The mixed economy of visible patrols in England & Wales, Bristol: The Policy Press.

Crawford, A. and Newburn, T. (2002) 'Recent developments in restorative justice for young people in England and Wales', British Journal of Criminology vol 42, pp 476-95.

SECURITY DESIGNS AND INTEGRATION PROCESSES FOR CRIME PREVENTION IN RESIDENTIAL AND COMMERCIAL ENVIRONMENTS

Adebayo Akinade, dfisn and Ademola Omoegun

ABSTRACT

Criminality and insecurity keep mounting daily, mostly in residential and commercial environment. With a continuous growth in residential and commercial centres, it is expected that secured communities be stimulated to ensure a comfortable and liveable environment for the residents and occupants. This however remains one of the principal challenges bedevilling the Nigerian urban centre, which then reduces individual's desirability to live in residential and commercial centres in the urban areas. Crime is a social problem in the society adversely affecting thousands of people in the residential and commercial communities. Serious crimes against persons and properties generate considerable fear within such communities. Crimes like theft, break-in, rape, kidnapping, banditry, robberies and murder are serious threats to the safety of communities. The resulting fear of crime in itself can restrict people's freedom of movement and prevent them from fully participating in the various activities in the communities. In particular, some groups of people are more vulnerable to crime and the fear of crime for example, older people, women, parents, teenagers, youth etc. Many different strategies are needed to combat the complex issues of crime in residential and commercial environment. A whole range of responses involving strategies in design, community action and law enforcement would be required to achieve successfully the objectives of crime prevention programmes. In this connection, there is a widespread acknowledgement that planners, architects, developers, security and law enforcement agencies and members of the communities including resident visitors can play an important role in enhancing the safety of our residential and commercial communities as they have a major influence in the design of the built environment. This paper endeavours to study the security level of residential and commercial environment in urban centres. The paper will examine criminality, insecurity and the security design and integration system within urban centres for better safety and proffer solutions. The purpose of this paper is to raise awareness of stakeholders, security and law enforcement agencies, developers, architects and town planners on the concepts and principles of CPTED. CPTED seeks to enhance the safety of developments and minimise the opportunities for crime to be committed.

Key terms: Security Challenges, Residential and Commercial Environment, Technology and Scientific Solutions

1.0 INTRODUCTION

There has been a high level of unprecedented criminality and insecurity in the country. This is one of the most prevalent problems existing in residential and commercial communities. Insecurity and criminality have caused negative influence on individual's mental, physical and social activities and also the vitality of their communities in terms of security and safety (De Biasi, 2017). A review documentation made by United Nations in 1990 in (Olajide and Mohd Lizam, 2017) revealed that while developed countries spend 2% to 3% of their annual budget on crime prevention and security of lives, 9% to 14% of the developing countries' annual budgets goes to such activity. This justifies the current situations within such developing economies with African continent inclusive. Having threatened both the local and the national security, this has impelled a huge allocation been channelled by the Nigerian government to the nation's security from the country's national budget (Achumba and Akpor, 2013).

According to the 1999 Federal Republic of Nigerian Constitution, "security and welfare of people stands as one of the main purposes of the government existence". However, this constitutional responsibility has long failed in placing a safe and secured environment for properties, lives, individual daily operations and economic events except for those in government's high-ranking positions who are usually guided by all sort of security (Okonkwo et al., 2015). More so, these high rate of insecurity and criminality have increased the terrorism, banditry, robberies, kidnapping and crime rate in different states of the country. The crime rate across the country keeps breeding destruction of properties and lives as well as increasing fear of crimes and insecurity. This then leaves revolting consequences for people, business and economic growth as activities such as foreign direct invest and international organisations wishing to invest in the country's economies and business are being discouraged.

Crimes involving robberies, car-snatching, kidnapping, vandalism or theft in properties are the most common forms of urban violence in Nigeria. Burglary, house and store breaking and other forms of crimes involving property rank second to larceny. It can be observed here that these crimes against property have no spatial preference, are not area specific and are perpetrated in rich and poor areas as well as in planned and unplanned areas. Property experts are able to show that the loss of life is highest in low-density residential areas while the loss of property is highest in medium density areas.

The major discussions in housing, safety and crime are rooted in the seminar work of Oscar Newman's *Defensible space* concept, (Newman, 1972) in Environmental Criminology and in an aspect of Environmental Psychology called territoriality (ef. Gifford, 1997). They are based on the premises that architectural and urban form does not cause behaviour, but that opportunity is inbuilt to the environment, potentially increasing or decreasing the likelihood of certain forms of behaviour occurring (Samuels, 1994:6). Crime is most likely to occur when potential offenders come into contact with a suitable crime target, where the chances of detection by others are thought to be low and the crime site lacks a natural guardian (Taylor and Harrell, 1996).

2.0 BACKGROUND AND PROBLEM STATEMENT

Crime is one of the human security problems confronting humanity across the world. Nations have grappled to contain the rising incidence of homicide, armed robbery, and kidnap, drug trafficking, sex trafficking, illegal gun running and a host of others.

Events of the past few years show that the spate of crime has assumed a debilitating proportion and requires the intervention of policy makers in this regard. According to Osawe, crime portrays the inability of government to provide a secure and safe environment for lives, properties and the conduct of economic activities considering the alarming increase in criminal activities in Nigeria such as armed robbery, terrorism and other related crimes. Olanrewaju avers that crime relates to drug use which has the social consequence on students manifesting in various forms including assassination, kidnapping, lack of interest in education, armed robbery and other criminal offences.

It has been observed that a factor which motivates criminality is that availability of arms in the hands of illegal users, particularly civilians. For instance, Hull *et al* posit that the proliferation of arms contributes to conflict in two main ways namely: 'increasingly lethal firepower is likely to cause higher levels of destruction; and that augmentation of sophisticated weaponry creates a vicious cycle whereby competing militias engage in an arms race to gain dominance incapability.

A Third Report on Violence in Nigeria (2006-2011) by Nigeria Watch Database noted that the second main cause of violence is crime. This is heavily concentrated in commercial and residential communities in the South, especially in highly populated areas like Lagos and Port Harcourt. Yet the Middle Belt is not immune from armed robbery and banditry,

especially in Plateau State, which records higher crime rates. These statistics on the trend and patterns of violent and non-violent crimes are worrisome and needs urgent attention from a multi-dimensional approach by stakeholders involved in anti- crime crusade.

Criminality and insecurity rate in the country's cities which comprise of residential and commercial communities keep rising daily. With a continuous growth in commercial and residential estates, it is expected that secured properties be stimulated to ensure a comfortable and liveable environment for masses. This is then assumed to enhance the emotional stability of residents and citizens and produce high work force efficiency towards the promotion of the country's Gross domestic product. Considering the levels of residential and commercial environment security systems which ranges from simple to sophisticated, different security systems have emerged over the years across the globe such as trained security personnel, trained dogs, thermal cameras, high/electric fencing, vigilantes, fire/back to base alarm systems, panic buttons, surveillance equipment and wire, fire system, home automation, temperature, spikes floor and water sensors, CCTV monitors, video recorders, 24hours security guards, and any type of anti-intruder perimeter control systems (Radetskiy, et al., 2015). This however has not been fully employed in Nigeria owing to procurement cost, difficulty in installation or use as well as the unplanned nature of most residential and commercial environments. (Ajibola, et al., 2011) noted the inefficient security problem within the length and breathe of the country which has resulted into numerous crimes acts and loss of lives.

However, the insecurity and criminality levels in Nigeria cannot be over mentioned without being traced back to the early military rule ages when bulky quantities and quality weapons were shipped into the countries for military uses during and after the civil war. Some of these weapons however were high jacked by the civilians and then became their tools for mischievous acts shortly after the war such as; robbery attacks, kidnapping and hostage taking, killings of innocent minds and ritualism which is high across the country (Olabanji and Ese, 2014). Worthy of note is the 1999 constitution's provision for citizen's right which has been distorted due to government's incapability to curb insecurity thereby leading to various shapes of violence, religious vehemence, communal clashes and crime not just at the national level but more significantly at the state and local level, where innocent lives are daily destroyed. This has made citizens in residential and commercial environments to vacate their comfort zone in search for a secured environment which are less comfortable. This has also kept citizens off some public zones and their participation in some public activities.

3.0 LITERATURE REVIEW AND THEORETICAL FRAMEWORK ON CRIMES IN RESIDENTIAL AND COMMERCIAL COMMUNITIES

Scholars and social analysts have defined crime from different perspectives. As such, a general definition of the concept has eluded the academia for years. While Farmer Lindsay see crime as a category created by law, Elizabeth A. Martin provided a more comprehensive definition when she noted that crime or offence (or criminal offence) is an act harmful not only to some individual or individuals but also to a community, society or the state ("a public wrong").

Crime is traceable to the formation of groups by individuals who have related interests with the aim of having a strong network. For example, Babalola explains that "drug, cultism and terrorism have an inexorable nexus, one to the other. Once a person gets hooked to a particular brand of drug, he craves for it; he finds easy partnership in anyone that shares identical belief in that line of psychosomatic attitude. Together, they form groups with defined purposes. In the process of carrying out their concerted aspirations, they employ different kinds of weapons; broken bottles, knives and cudgels and recently guns and pistols. In addition, bombs have also become tools in the hands of armed robbers, militants and terrorists in most parts of the country who

take advantage of the explosives to break into banks, Automated Teller Machines, and also to attack religious institutions, hotels/restaurants.

The Classification of Crimes by the Trent Online

Available evidence from the Trent Online database reveals that the following violent and non-violent crimes exist in Nigeria with different scales of violent incidents since 2013 when it became operational.

State	Crime	Number Of Occurence	No. of Fatalities
2015			
Lagos	Rape	2	2
	Drug trafficking	1	
	Cultism/murder	3	
Plateau	Drug trafficking	1	-
Ondo	Rape, kidnapping, murder	3	1
	Bank robbery	-	-
	Currency counterfeiting	-	-
Edo	Robbery	1	5
Bauchi	Robbery, ritual murder, kidnapping	1	-
Kwara	Homicide	1	-
Taraba	Homicide	1	-
Abia	Homicide	2	1
Imo	Homicide	1	1
2014			
Lagos	Rape, murder, drug trafficking	7	7
Kaduna	Murder	1	1
Ogun	Rape, ritual	4	19
Bayelsa	Kidnapping	2	1
Oyo	Robbery	1	2
Imo	Assassination, Arms	1	2
Zamfara	Proliferation	1	1
Osun	Murder	1	1
Plateau	Assassination	2	9
Ekiti	Murder, rape	1	1
Bauchi	Rape	1	-
Kogi	Rape	1	-
2013			
Ebonyi	Child trafficking,	1	-
Lagos	Rape, car theft, ritual murder	4	-
Abuja	Fake UN recruitment	1	-
Akwa Ibom	Child trafficking	1	-
Total		**47 Events**	**54 Fatalities**

Trent Online statistics in Table 1 reports 54 deaths in 47 criminal events across the states between 2013 and 2015. Fatalities spread across many states of the federation with varied intensity due to some demography variable. In Lagos, the confrontation between security forces and drug traffickers led to four deaths involving the traffickers in 2014, while ritual murder produced 18 deaths the same year. Also in Lagos, rape occurred four times as

reported by the Trent. In Ogun State one of the rape cases did not lead to any death, while the only incident of 'gang rape' led to the death of the victim. The alarming rate of ritual killings in Ogun also led to 18 deaths in 2014. While rituals and murder produced the highest number of fatalities, rape occurred more than other crimes between 2013 and 2015.

The Trent online database reveals that there are two classifications of crime, namely violent crime and non-violent crime in the country. For instance, while fake UN recruitment syndicate who was arrested by the police in Abuja in January 2014, and the arrest of four men at Lagos airport in December 2013 can be described as non-violent crimes, street beheading for ritual purposes and ritual murder of a virgin in Lagos are classified as violent crimes. However, there were cases where culprits robbed and gang raped their victims thereby inflicting pains on them. Such attacks can be described as violent although not fatal. Fatal incidents are those that resulted in deaths. Where an incident involves robbery, victims usually lose their valuables after the attack like the 2014 incident in Ogun State where a businesswoman lost N1,803,000 cash, gold worth N200,000 and wrist watch worth N5,000 and blackberry phone at a total sum of N2,187,500to armed robbers.

In addition, drug trafficking has also been a source of violent crime just like the 8 January, 2014 incident in Mushin area of Lagos where four traffickers were gunned down by security operatives when they opened fire on the men of the National Drug Law Enforcement Agency (NDLEA). It shows that drug traffickers motivate arms proliferation. Most of the crimes reported in the country have in one way or another denied people their rights to freedom of movement, right to ownership of property and other socio-economic rights. Law enforcement agents have also been punished for crimes especially rape and complicity in arms proliferations that aided robberies.

The fact that rape and armed robberies have become the dominant crimes in the country cannot be disputed as they are more prevalent than others like unlawful possessions of firearms, cultism, car snatching and homicide in industrial, commercial and residential communities.

Armed Robbery in Residential and Commercial Communities

Armed robbery has remained a major cause of death in Nigeria. Victims cut across socio-economic status and occur mostly in major cities and states along transit points. Also, security personnel, civilians and robbers themselves have fallen prey to armed robbery. An overall 4,268 deaths occurred in 1682-armed robbery incidents nationwide. There were reports of fatal armed robbery incidents in all the states in Nigeria including the Federal Capital Territory, Abuja.

However, fatalities varied by states. An emerging trend in armed robbery is bank attacks. In March, 26, several people including a branch bank manager and his Assistant were killed during an armed robbery incident in Oyo State. This attack came barely two months after a bank was attacked in Ondo and 22 people including policemen and civilians were killed. The most fatalities were reported in Delta (946 deaths), Lagos (819 deaths), Anambra (225 deaths), Ogun (184 deaths) and Zamfara (160 deaths). Gombe, Bayelsa, Jigawa, Kebbi and Plateau, on the other hand, enjoyed low fatalities from lethal armed robbery incidents. There were 13 deaths in Gombe, 16 in Bayelsa, 18 deaths in Jigawa and Kebbi respectively and 21 in Plateau. These statistics show that less fatal armed robbery incidents occur in Northern part of Nigeria that their Southern counterparts.

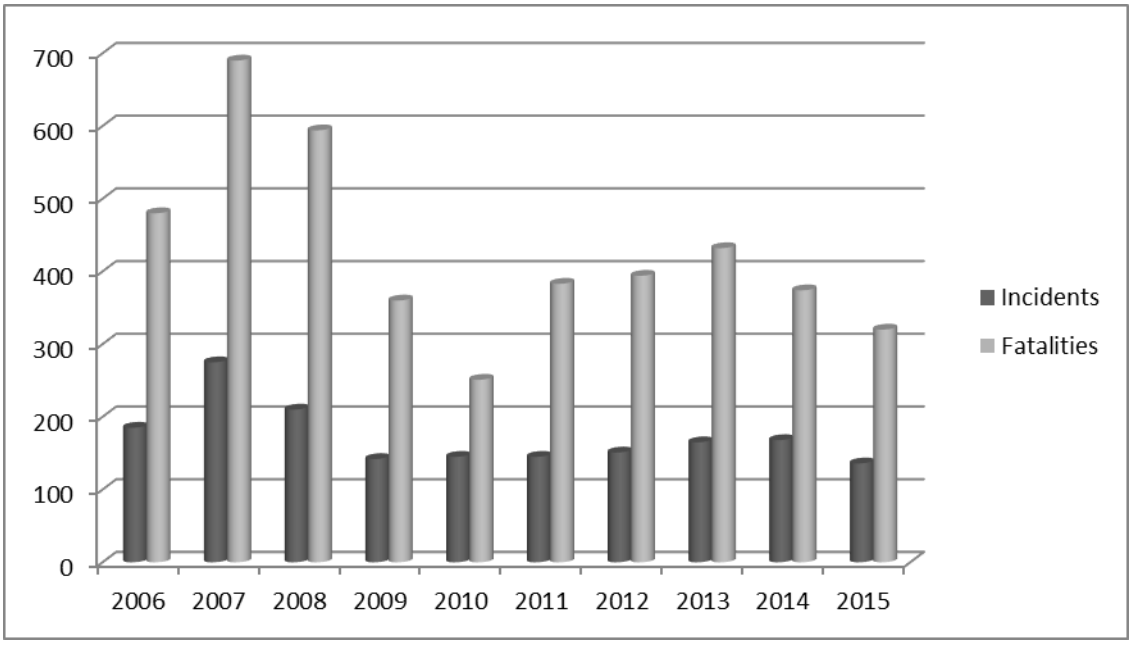


Figure 1: Yearly Trend of Armed Robbery Fatalities and Incidents (June 2006 – September, 2015)

Figure 1 shows the trends of robbery fatalities in Nigeria between June 2006 and September, 2015. Results show that there were reported 275 robbery incidents that culminated into 690-deaths in 2007.

This marked the most fatal year in relation to fatal robbery incidents within the period under review. The trend changed in the subsequent three years (2008-2010) with a downward trend. About 594 deaths occurred in 210 robbery incidents in 2008; another 360 deaths in 142 incidents in 2009 and 251 deaths in 145 incidents in 2010. However, fatality trend has fluctuated between 2011 and 2015. In 2011, about 383 deaths occurred in 145 robbery incidents, 394 deaths in 151 incidents in 2012 and 432 deaths in 165 in 2013. Year 2014 marked a drop in robbery fatalities (374) from the previous year but still maintained the upward trend in the number of incidents with 168 incidents. Year 2015 remains unpredictable when it comes to the number of robbery incidents and fatalities. However, with the 320 deaths in 136 deaths within ten (10) months of 2015, one may argue for high incidents of armed robbery cases as well as increase in the number of robbery fatalities.

Cultism in Residential and Commercial Communities

Cult related activities abound in the nooks and crannies of our society especially in institutions of higher learning. Worrisome it has become that such cult activities have been taken to secondary schools though not as pronounced as in the higher institutions. Cultism is rampant among teenagers and young adolescent youths. Casualties of cultism cut across innocent civilians, gang members and security personnels. Cult attacks in the month of September saw the killing of 61 people in three states. In Rivers states, 20 persons were brutally murdered during a clash between Degbam and Barbeach Groups said to be the armed wing of Islander. In Edo State, 25 people were killed in a cult clash between Manfight and Aiye (Neo Black Movement of Africa) over supremacy battle. Cultists also saw the killing of 16 people during a clash between 'Aiye' and 'Eiye' cult confraternities.

A breakdown of the figures shows that there were 2363 deaths from cult related activities in 28 states of the federation. Rivers State was most hit with cult killings with 765 deaths. There were 323 deaths in Lagos State, 306 in Edo, 202 in Delta, 104 in Bayelsa and 99 in Ogun. Most affected states are from the Southern part of the country. On the contrary, least affected states include Sokoto and

Katsina with 1 death respectively, Plateau and Bauchi with 2 deaths respectively and Oyo with 4 deaths. Oyo State remains the only Southern state that has relatively been free from cult related killing. With the statistics, one can argue that there is less cult killings in the North than in the South of Nigeria.

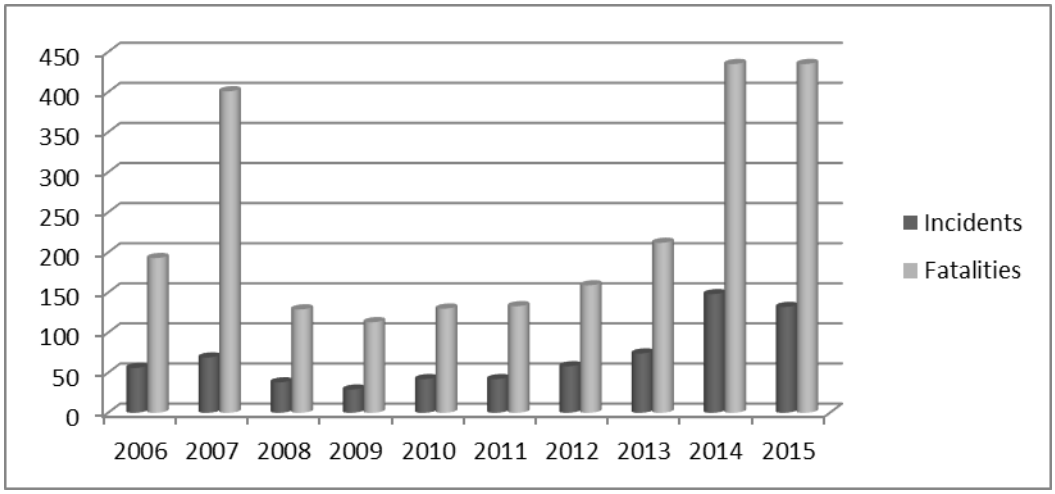


Figure 2: Yearly Trend of Cult Killings and Incidents (June 2006 – September, 2015)

Yearly mapping of cult killings in Nigeria between June 2006 and September, 2015 shows that fatality record between January to September, 2015 has already equalled the 2014 record of cult killings. There were 435 cult related deaths in 2014 and 2015 (January to September). While such deaths occurred in 148 incidents in 2014, there were 132 cult related fatal incidents in 2015. In 2007, about 401 people were killed in 69 cult incidents and another 212 people killed in 74 incidents in 2013. About 193 people died in 56 cult incidents between June and December, 2006; 159 people were killed in 58 incidents in 2012; 133 killed in 42 incidents in 2011; 129 killed in 38 incidents in 2008 and 113 killed in 29 incidents in 2009. Therefore, year 2009 recorded the least fatalities and number of cult incidents within the period under review.

Kidnapping in Residential and Commercial Communities

Kidnapping has remained one of the major crimes in the nation. Abati noted that kidnapping has become a national phenomenon as the entire country is now a kidnappers' den. According to him, ransom kidnapping and hostage taking are no longer restricted to the Niger Delta area, or South-South of Nigeria with reported cases in Lagos, Abuja, Benin City, Owerri, and now Kaduna and Kano. Statistics in Table 2 shows that kidnapping has spread to 22 states of the Federation, with a total 457 deaths in 166 events. Abia recorded the most cases of fatal kidnapping with 55 deaths, seconded by Lagos with 50 deaths, Delta with 44 deaths, Rivers with 25 deaths and Borno with 20 deaths. Four of these states are from the Southern part of Nigeria. Victims of kidnapping spans wide including security personnel as severally witnessed in Obingwa, Abia state, kidnapped foreign and national residents and the kidnappers themselves. Often times, ransom is paid to secure the release of the abductees. However, incidence of kidnapping in Borno was perpetrated by Boko Haram, an Islamic extremist group that busted in limelight in 2009. In February, 2013, scores of lives were reportedly lost in connection with the search of French hostages kidnapped by Boko Haram in Dikwa. There were instances where some women were kidnapped, raped and killed afterwards. For instance, a businessman Shola Olaseinde was kidnapped and killed by 5-gang fraudsters impersonating as women on a dating site in Rivers State. In 2010, another woman, Hyacinth Azu Nwangolo, Head of Economic Affairs, Rivers State Ministry of Women Affairs was abducted in her car and

killed after ransom was not paid to secure her release. Another goring incident happened in Edo State in 2012 when two students of the Federal Polytechnic, Auchi, Edo State, Henry Edewo and Emmanuel Isikhuime, kidnapped, rape and murder a female student, one Mercy Peter also a student of the institution. They bury their victim in a forest. The victim, who was kidnapped on July 29, that year, was killed four days later after she was serially raped by the suspects. They were also alleged to have continued to demand for ransom from her parents after killing her.

While kidnapping thrived in some states, others recorded fewer fatalities and incidence of kidnapping. Such states include Benue, Bayelsa and Bauchi with 1 death respectively, Taraba and Ebonyi with 2 deaths each. There was only one incident of kidnapping that resulted into 1 death in the Federal Capital Territory (FCT).

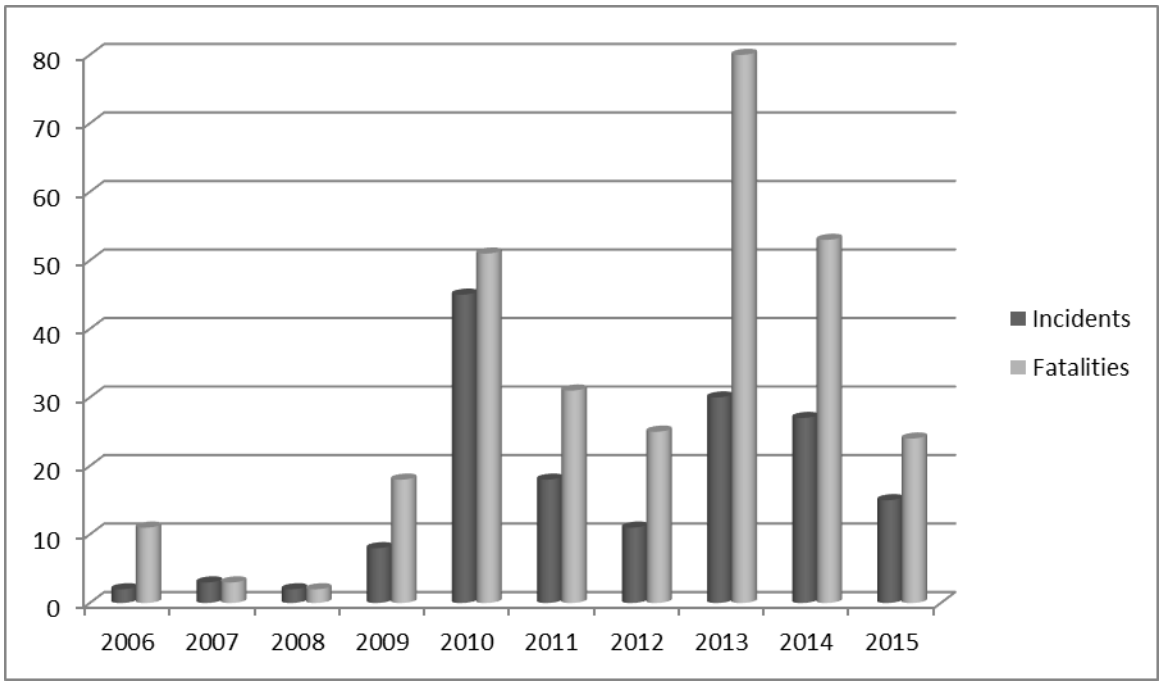


Figure 3: Yearly Trend of Kidnap, Fatalities and Incidents (June 2006 – Sept ember, 2015)

Year 2013 was reported the most fatal with 80 deaths from 30 kidnap incidents. There were fewer kidnap fatalities and incidents in 2014 as 53 deaths were recorded in 27 incidents. In 2010, 51 people were killed in 45 kidnap incidents and another 31 people killed in 18 incidents in 2011. About 25 people were killed in 11 incidents in 2012 and 18 killed in 8 incidents in 2009; 11 killed in 2 events in 2006; 3 killed in 3 events in 2007 and 2 killed in 2 incidents in 2008. Between January and September, 2015, 24 people have been killed in 15 kidnap incidents nationwide.

Security personnel were the most hit in the overall kidnap incidents in Nigeria. About 621 security personnel comprising of the police, soldiers, naval officers and secret service men were killed in the various kidnap incidents. This figure overshadowed the number of kidnappers and civilians killed. In Abia State, security personnel were severally targeted and killed by kidnappers and their riffles taken always for further attacks.

Domestic Violence in Residential and Commercial Communities

Domestic violence had become a national calamity due to its national coverage. Domestic violence is widespread and shows no signs of lessening in Nigeria. The CLEEN Foundation reports 1 in every 3 respondents admitting to being a victim of domestic violence. The survey also found a nationwide increase in domestic violence in the past 3 years from 21% in 2011 to 30% in 2013. Social

commentators and analysts have narrowed down to the main causative factors of domestic violence to include drunkenness, financial issues, and the rejection of a partner's sexual advances. An instance of drunken motivated domestic violence was captured in an incident where a young man, (Ibrahim Sanni Mai-Gunjo) murdered his father with a machete, after accusing him of being a drunkard. Women often face physical violence at the hands of their family members. The most common forms of physical violence include rape, murder, slapping, and kicking.

Statistics in Table 2 shows that there were 608 deaths in 546 domestic incidents in 34 states of the federation and FCT, Abuja. Lagos State had the most cases of fatalities from domestic violence as it recorded 121 deaths in 120 incidents. This may be argued from the perspective that it has one of the highest populations in the country. Other states with high fatalities from domestic violence include Delta (52 deaths), Edo (32 deaths), Ogun (29 deaths) and Oyo (27 deaths).

On the contrary, some states recorded insignificant number of deaths from domestic violence. These states include Adamawa, Gombe and Sokoto (2 deaths respectively), Taraba (4 deaths) and Jigawa (5 deaths). These statistics shows that domestic violence is more rampant in the South than in the North and this assertion corresponds with the 2008 Nigeria Demographic and Health Survey (NDHS) data on Women's Experience of Violence which reported that domestic violence cuts across all socio-economic and cultural background and 28 per cent of all women, almost a third of all women in Nigeria, have experienced physical violence, a significant number in a country of almost 160 million, where almost half are women.

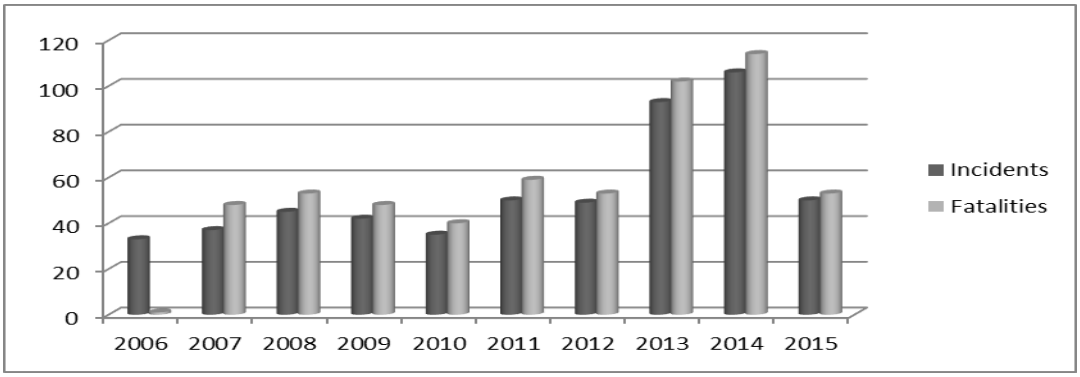


Figure 4: Trending Fatal Domestic Violence by Year

Statistics in the table above shows that there were more domestic violence related deaths in 2014. About 114 people including children, teenagers, and adults, both male and female lost their lives in 106 incidents. There were further 102 deaths in 93 incidents in 2013; 59 deaths in 51 incidents in 2011; 53 deaths in 2008, 2012 and 2015 (January to September) respectively. While 2009 recorded 48 deaths, 2007 and 2010 recorded 40 deaths respectively. The least deaths in domestic violence occurred between June and December, 2006.

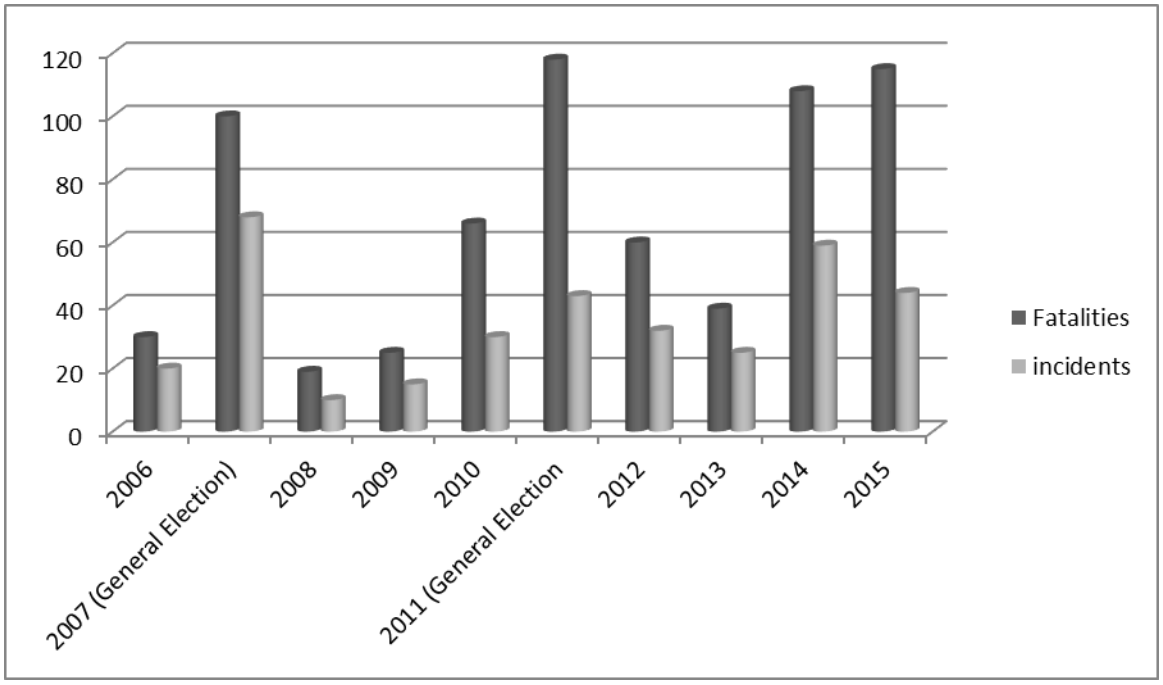


Figure 5: Assassination/ Thuggery/ Hooliganism in Residential and Commercial Communities

Assassination has been a major cause of fatal deaths in Nigeria. About 676 persons were assassinated in 35 states in Nigeria and FCT, Abuja. Assassinations are often targeted at prominent persons especially politicians and perpetuated by thugs and hooligans. Many people were assassinated during general elections. Lagos State witnessed the most reported cases of assassinations with 172 deaths between June 2006 and September, 2015. About 67 people were killed in Oyo State, 42 persons in Bauchi and 32 persons in Delta, Ogun and Rivers states respectively.

The assassinations mainly occurred at the different stages of the general election including the pre, during and post-election periods. Figure 8 shows a unique pattern of assassination during the 2007, 2011 and 2015 general elections in Nigeria. About 102 people were assassinated in 56 violent events in 2007, 118 persons in 43 events in 2011 and 115 persons in 44 events in 2015.

Residential Estate Security

Security is a prominent phenomenon which everyone needs to guarantee their comfort and safety, Azid and Kumar (2011). Similar to health, residential security is an essential feature of human life, hence, different technological developments have emerged across the globe to aid security of life; asset and privacy at all times, Budijono et al (2014). Where crime exists, individual desires proper measures to prevent intrusions or damages to their lives and properties. This involves the prevention of unauthorised access or damage to residential environment and lives. In developed countries the use of wireless communication devices keeps increasing in preventing crime through quick action; image capturing and sound recording to display remote places; protection of child's safety through authorisation and authentication systems efficiency in communication. This relates to wireless communication tool in storing and viewing of data on internet. However, security measures in developing countries such as Nigeria are commonly applied through the erection of high walls across the buildings or through other means such as provision of dogs, vigilante groups and so on without much application of advanced security systems.

In the work of Agboola 1997 cited in Olajide and Kolawole, (2013), the most noticeable form of providing security around residential

property is through the erection of high walls which mostly obstruct the beautification of such properties. Noteworthy is that bringing this together with burglar proof in shielding houses, erection of huge gates and sturdy locks, presence of lighting facilities across houses and other protective devices, there is strong indication that Nigerian's city Architecture is governed by the fright of robber's invasion. Agboola then suggested that such actions offer an invitation to robbers rather than protecting the occupiers. Further, this over the years have caused the death of several families within Nigeria at large owning to the fact that design nature of houses often deters rescuers whenever there is inferno or other negative event around the houses mostly at night. Among the recommendations offer by Agboola include; the aiding of neighbourhood association, high consciousness of resident; organisation of vigilante groups; as well as urban designers and planners being security conscious while dealing with residential neighbourhoods work to keep the general environment healthy and accessible.

Residential Alarm monitoring has also become one of the keys professionally recognised home security instrument, which engages in any number of devices and policies to ensure safety around property Olajide and Kolawole, (2013). Hence, the understanding of its operation and the component that makes a good monitoring company will aid the satisfaction of safety choices that will deliver value to end users (occupiers) (Hannah, 2011). According to Hannah, modern security devices can prevent possible crime acts and any actual damaging effort. Additionally, Khanna and Omprakash, (2011), also posited that where individual want to secure their lives and properties from crime, the need to introduce a single mobile device to cover the entire proficiency and functionality of home security cannot be underestimated, as the incorporation of different parts and their solution can be established through current and up-to-date application and devices, to aid the safety of lives and property. Subsequently, Azuh (2012) in his work on safeguarding of homes through affordable security systems posit that affordable home security devices can keep criminals away. Although some believe that only the rich obtain these security devices owning to its high cost, Azuh however oppose this affirming that there exists some affordable and effective security gadget which the low-income class can purchase. He therefore posited that door step alarm and camera home security system as one of the effective low-cost security devices. Where camera home security system functions like a closed-circuit television (CCTV), it, according to the home security system.org helps in deterring criminals while significantly adding to entire security system when mounted at an easily noticeable spot around a house. Other low-priced security system recognised by the author is: mini magnetic contact alarms; combination lock and electronic watch dog; stickers and home security yards sign.

4.0 STRATEGY ON CRIME PREVENTION FOR RESIDENTIAL AND COMMERCIAL COMMUNITIES

Security Challenges and Solutions

Safety and security touch upon all aspects of human life in residential and commercial communities. Cities and town suffer from increasing social and economic challenges, as well as paralysis caused by fear and mismanagement. In the face of increasing urbanisation and globalisation, the police and other security agencies, cannot effectively address the problem of insecurity that threaten people's lives and property.

Insecurity cannot be reduced by solving issues of crime and violence simply. Crime and people's anxieties about crime and violence are catalysts for feeling of insecurity with regard to quality of life. Fear of violence has come to symbolise all other fears: economic and social impoverishments, ethnic and cultural conflicts, domestic violence, thuggery, vandalisation, assassination, kidnapping, etc.

Community safety, on the other hand, is a basic human right as entrenched in the constitution. It is a public good that determines quality of life. Many factors negatively influence people's sense of community safety. Everyone has a responsibility to make communities safer. No single agency can address crime and safety

problems on its own. Crime prevention and community safety strategies need to be adapted to local needs on the basis of good analysis and targeted plans. Adequate capacities need to be built at the local level, including those for the measurement of progress and performance.

Security challenges are becoming more complex and a plethora of various actors are attempting to play a role in addressing security problems. There is an attempt to broaden the focus to include the security of people; so, called "human security" which means protecting vital freedoms. Protecting people from critical and threatening situations, building on their strengths, demands an integrated approach. Human security connects different types of freedoms - freedom from want, fear and freedom to take action. To achieve these freedoms there are two general strategies: **protection** and **empowerment.** Protection requires effort to develop norms, processes and institutions that systematically address security problems. Empowerment enables people to become full participants in decision-making. Protection and empowerment are mutually reinforcing, giving people the building blocks of survival, dignity and livelihood and enabling people to participate in governance and make their voices heard. From an urban development perspective this requires building strong institutions, establishing the rule of law and empowering people.

Crime, violence and insecurity present major challenges for the social and economic development of cities and towns. Delinquency and violence in urban areas is no longer viewed exclusively as a criminal problem but also as a real developmental problem. Insecurity contributes to the isolation of groups and to the stigmatisation of neighbourhoods, particularly those concerning the poor and more vulnerable. It creates conditions of fear, hinders mobility and may be a major stumbling block for participation, social cohesion, and full citizenship. Furthermore, insecurity erodes the social capital of the poor and the social fragmentation results in a decline in social cohesion and an increase in social exclusion. Social exclusion prevents certain groups from equal and effective participation in the social, economic, cultural, and political life. There is a close connection between social exclusion and poverty. Most of the excluded groups - e.g. women, children and youths, the elderly, widows, and AIDS sufferers - are cut off from networks that provide access to power and resources, making them vulnerable and increasing their risk of being poor. The vicious cycle of poverty leads to social stigmatisation and marginalisation from institutions, leading to greater poverty, having a profound negative impact on quality of life.

At the community level, social cohesion is an asset that provides security, regulates behaviour, and improves the standard of living of the community as a whole. Social cohesion and civic engagement are preconditions for better schools, safer streets, faster economic growth, more effective government, and healthier lives. This is why crime prevention strategies must be focused on enhancing social inclusion, and engaging marginalised groups as assets, not treating them as liabilities, within their communities. Within their meaningful engagement and active involvement, crime prevention strategies will be less effective.

Two general approaches can be utilised to advance the security of people. On the one hand, government can increase protective measures such as police manpower, prison sentences, and "zero tolerance" measures, which include curfews for minors or the lowering of the age of legal responsibility.

On the other hand, government can employ prevention-based strategies which involve the decentralisation of the fight against insecurity through the delegation of police responsibility either to local authorities or civil society associations or both. Local authorities have a key role to play in providing safety to their inhabitants, not only because it is stipulated in law, but local governments are accessible and accountable to the people, and they provide services to the people.

5.0 CRIME-PREVENTION PROGRAMMES IN RESIDENTIAL AND COMMERCIAL COMMUNITIES

There are a number of crime-prevention programmes set up in residential and commercial communities to help deter and detect crimes. These programmes are supported and often headed by members of the communities in conjunction with security and law enforcement agencies. The programmes are as diverse in nature as they are in number, yet they complement one another.

(i) Neighbourhood Watch Programme

A Neighbourhood Watch Programme is an organised network of citizens interacting with other neighbours and the police in preventing and detecting crime in their neighbourhood. Law enforcement efforts to reduce crime cannot be accomplished effectively without the support and cooperation of all citizens. A strong community involvement with neighbours helping themselves and other neighbours in becoming more alert to criminal activities in the neighbourhood, protecting their property, and reporting suspicious activities is essential to an effective crime prevention programme.

A Neighbourhood Watch Programme is designed to encourage security service members and their families to actively participate in protecting their own property and the property of their neighbours, joining community crime-prevention programmes, and reporting suspicious activities to police officers. The programme is designed to develop the following:

- The awareness of community crime trends and prevention efforts;
- The knowledge of quarters' security procedures;
- A cooperative system of surveillance over each neighbour's property;
- Accurate observation and reporting of suspicious activities;
- The establishment of a reliable, two-way information link between the community and MP forces.

Most neighbours know the routines of the other families that live near them. They know what cars are normally parked in the neighbourhood and when families are on vacation or out of the area. Neighbours are in a very good position to recognise burglars and other intruders. Also, residents are in a good position to recognise safety hazards and crime-conducive conditions near their homes.

Models for Neighbourhood, Vigilante Scheme and Community Security

A neighbourhood watch or called a crime watch or neighbourhood crime watch, is an organised group of citizens devoted to crime and vandalism prevention within a neighbourhood. In the United States it builds on the concept of a *town watch* from Colonial America.

Neighbourhood watch (also known as block watch, apartment watch, home watch and community watch) grew out of a movement in the US that promoted greater involvement of citizens in the prevention of crime (Titus, 1984). A neighbourhood watch may be organised as its own group or may simply be a function of a neighbourhood association or other community association.

Neighbourhood watches are not vigilante organisations. When suspecting criminal activities, members are encouraged to contact authorities and not to intervene.

The Neighbourhood Watch scheme in the United Kingdom is a partnership where people come together to make their communities safer. It involves the Police, Community Safety departments of local authorities, other voluntary organisations and, above all, individuals and families who want to make their neighbourhoods better places to live. It aims to help people protect themselves and their properties and to reduce the fear of crime by means of improved home security, greater vigilance, accurate reporting of suspicious incidents to the police and by fostering a community spirit.

The Theory of Neighbourhood Watch

The most frequently recorded mechanism by which neighbourhood watch is supposed to reduce crime is by residents looking out for suspicious activities and reporting these to the police. The link between reporting and crime reduction is not usually elaborated in the literature. However, it has been argued that visible surveillance might reduce crime as a result of its effect on the perceptions and decision making of potential offenders.

Hence, watching and reporting might deter offenders if they are aware of the propensity of the local residents to report suspicious behaviour and if they perceive this as increasing the risks of being caught.

It is also feasible that neighbourhood watch might reduce crime through the other components of the programme package. It has been argued that property marking might lead to a reduction in crime as a result of making the disposal of marked property more difficult (Laycock, 1985). This might reduce offending rates if potential offenders viewed marked property as increasing the risk of detection. Home security surveys might lead to a reduction in crime as a result of making it physically more difficult for an offender to enter the property (Bennett and Wright, 1984).

Objectives of Neighbourhood Watch

- To prevent crime by improving security, increasing vigilance, creating and maintaining a caring community and reducing opportunities for crime by increasing crime prevention awareness.
- To assist the police in detecting crime by promoting effective communication and the prompt reporting of suspicious and criminal activity.
- To reduce undue fear of crime by providing accurate information about risks and by promoting a sense of security and community spirit, particularly amongst the more vulnerable members of the community.
- To improve police/community liaison by providing effective communications through Neighbourhood Watch messaging systems which warn Co-coordinators of local crime trends which they can disseminate to their scheme members, and by members informing the police of incidents when they occur.
- Encourage vigilance amongst scheme members and actively encourage the early reporting of suspicious incidents to the police.
- Receive crime information from the Neighbourhood Watch messaging system and distribute these messages to scheme members.
- Encourage scheme members to be aware of and put into practice crime prevention measures, such as property marking and security devices.
- Keep a check on vulnerable households and provide advice to members about dealing with callers at the door.
- Circulate newsletters and other relevant information to scheme members.
- Welcome newcomers to the neighbourhood and invite them to be part of the scheme.
- Supply each scheme member with Neighbourhood Watch and crime prevention literature, such as Neighbourhood Watch window stickers and incident report cards.

6.0 SPECIALISED PATROL TACTICS AND SURVEILLANCE IN RESIDENTIAL AND COMMERCIAL COMMUNITIES

Specialised patrol operations use a variety of tactics in attempting to control identified crime problems. The most common tactics include uniformed tactical patrols and suspect and area surveillances. The following paragraphs discuss these tactics in terms of their target crimes, operation requirements and characteristics, and established or perceived levels of effectiveness.

The appropriateness of a given tactic depends on the characteristics of a particular crime problem. The selection of specialised patrol tactics should be made on the basis of a careful and continuous analysis of crimes. Most crimes can be addressed by more than one

tactic. Several tactics might be tried in an effort to find the best one, and it is quite possible that the most effective approach to a given crime problem will include the combination of several tactics.

(i) Uniformed Tactical Patrols

A uniformed tactical patrol is the most traditional and widely used form of specialised patrol. It is a simple, straightforward approach to specialised patrol that involves the same procedures and techniques used by police officers on routine patrol. These include constant visible movement throughout an area to generate a sense of police presence, careful observation of street activity, vehicle and pedestrian stops, and citizen contacts. The difference between uniformed tactical patrols and routine patrols are that uniformed tactical patrols use these tactics in an intense, concentrated fashion. Patrol officers are relieved of the responsibility for responding to routine calls for services so that they can devote their full time and attention to patrol, thus intensifying its impact. In addition, uniformed tactical operations typically deploy a number of police officers in target areas, thereby increasing the level of patrol in these areas.

Uniformed tactical patrols can be used to control virtually any type of suppressible crime (for example, crimes that can be viewed from locations where the police have a legitimate right to be and those that can be potentially affected by police operations). These suppressible crimes include street robberies, purse snatches, vehicle thefts, burglaries, and housebreakings. Uniformed tactical patrols can also have an impact on other types of crime as officers use observation, field interrogation, and citizen contacts to develop information on the locations, activities, vehicles, and associates of suspects.

The primary purpose of uniformed tactical patrol is deterrence. This tactic is based on the assumption that highly visible, active patrols will deter potential offenders. By increasing the perceived probability of apprehension, conspicuous patrol is thought to reduce the likelihood that crimes will occur. If the deterrence should fail, heightened patrol coverage is believed to increase the probability of the immediate apprehension of the suspects.

Uniformed tactical patrols are often used to saturate an area that is experiencing a particularly serious crime problem. Although it has been widely used for years, saturation patrol has never been clearly and adequately defined. Exactly what level and intensity of patrol constitutes saturation has never been determined, nor have the effects of different levels of patrol been clearly established. It is difficult to prescribe the level of uniformed tactical patrols that should be used to disrupt a crime pattern in a particular area. This should be determined through an analysis of the size and characteristics of the area of concentration of each potential target crime pattern coupled with an assessment of manpower availability.

This is sufficient to saturate the primary locations of the target crimes during the high-crime hours, and it will lead to a substantial reduction in these crimes with little apparent spill over into adjacent areas.

(ii) Area Surveillance and Intelligence

Covert patrol and surveillance of high-crime areas can be used to make apprehensions for crime problems. These problems include those for which there are no suspects who warrant personal surveillance, the suspects are too numerous to permit personal surveillance, and there are too many potential targets to conduct either physical or electronic stakeouts. Examples of these types of problems would be a rash of residential burglaries or auto thefts in a particular area.

This tactic simply involves the covert patrol of a particular area and the observation of suspicious or unusual activities and occurrences that might indicate the likelihood of a crime. Suspicious individuals are not stopped but are watched until they either commit an offence or the officers' suspicions are removed.

The list of various techniques that can be used in an area surveillance is virtually endless. The following are some techniques that have been effectively used by specialised patrol units:

- Mingling with citizens at the crime scene to pick up information on possible suspects;
- Maintaining rooftop surveillance of a shopping centre's parking lot to locate larcenies from vehicles;
- Surveillance of housing areas by posing as maintenance workers;
- Following likely crime victims such as elderly citizens leaving a bank;
- Surveillance of rooftops for unusual activity from aircraft or higher buildings. Binoculars are used to facilitate surveillance, and rooftops are marked so that street units can be dispatched to check out suspicious circumstances.

As in all types of plain or uniformed patrol, care should be taken to ensure that area surveillance is truly covert. Rental vehicles that can be changed frequently provide an excellent, though expensive, means of covert transportation.

Police on covert patrol should be dressed to blend in with the environment in which they are working, and they should have apparently legitimate, non-police related reasons for being where they are. Several specialised units have found that surveillance teams composed of one male and one female officer can work in many situations without arousing suspicion. An apparently married or romantically involved couple lingering in a park, meandering slowly down the street, or sitting together in a parked car would generally appear less suspicious than two male MP Officers doing the same things. Finally, it should be noted that in some small neighbourhoods where residents know each other well, covert surveillance may be difficult, if not impossible, since the presence of any stranger arouses immediate curiosity and suspicion.

These tactics represent the basic approaches that specialised patrol operations normally take in trying to control suppressible crime. Some of the tactics (such as uniformed tactical patrols) are directed primarily at crime deterrence, while others (such as suspect surveillance) are used to achieve apprehensions for target crimes. The tactics are most commonly used independently of one another. However, there are some indications that the combined use of several tactics in an integrated operation might be an effective way of coping with particular types of crime. Especially promising is the coordinated use of highly visible and covert patrols. A visible patrol force could be deployed to a particular area to deter crime there and direct it toward other areas in which police forces using covert tactics are working. To date, efforts to direct criminal activity to areas or targets where police forces are set up to make apprehensions have only been tried on a sporadic basis. However, this appears to be a promising approach to crime control and warrants greater attention in the future. It can be viewed as the creative use of crime displacement.

7.0 SECURITY CHALLENGES IN COMMERCIAL ENVIRONMENT SECURITY

COMMERCIAL ENVIRONMENT SECURITY COVERS COMMERCIAL AND MERCHANTILE BUIIDINGS, SHOPPING COMPLEX, AND BANKING HALL: THREATS AND SOLUTION

Office buildings have large numbers of people interacting within the premises; however, most people on the property either work in the building and are known to others at the site or are there to conduct business and are on site for a limited time. From a crime prevention standpoint, the open and inviting nature of office buildings means that many people have ready access to the property, including an increased number of potential victims, as well as those with the motivation and knowledge to perpetrate crimes.

The concerns discussed may be addressed with measures alternative to an influx of security personnel during peak traffic times, and if properly enforced and maintained, can prove to reside closer to the property's needs rather than exercising overkill with excessive labour. Dependent on the results of the crime

analysis, a cost-effective crime prevention mixes of policy and procedure, physical security hardware, and Crime Prevention Through Environmental Design (CPTED) may be sufficient to alleviate hazards posed by the substantial population of known and unknown persons, and the openness of the facility. For most office buildings, regardless of the level of criminal activity, environmental changes can prove to be the panacea for the reduction of existing criminal elements and fear of crime, as well as the increased quality of life on the premises. CPTED can restrict access to unauthorised areas by way of natural barriers and means such as elevators that are visible from the lobby and that stop on public floors only with receptionists or other personnel stationed at the entrance. Crime deterrence may also come from increased visibility by proper maintenance of outdoor landscaping, the use of glass walls rather than bricks and mortar, and clearly marked restrooms visible from the lobby. In more complex environments not fully conducive to CPTED, CCTV systems may be viable options to increase area visibility. Though the costs of CCTV have dropped dramatically in recent years, the expense must be justified by an actual, not perceived need.

i. BUILDING

a) ***Problem:*** Unauthorised access

Solution: Close off the side entrance to all unauthorised personnel; establish a security checkpoint at the main entrance to check issued Identity cards for employees; and monitor sign-in registers for visitors who have obtained approval from the hosting tenant.

b) ***Problem:*** General security issues

Solution: Require the maintenance staff to make hourly inspections of the building; mandate that maintenance closets and electrical rooms be made off limits to all unauthorised personnel and be locked at all times; conduct quarterly crime prevention meetings to be attended by management and tenant representatives that are sponsored by the local law enforcement; and relocate the pay phones from the parking garage to a location inside the building and nearer to the lobby.

c) ***Problem:*** Personal security

Solution: Seek out martial arts instructor; offers discounted building space and subsidise self-defence classes for building tenants and employees who are interested in learning martial arts and general self-defence.

d) ***Problem:*** Improve the privacy of the offices located on the top floor

Solution: Lock the staircase doors to the top floor (permitting exit only through the stairs from the top floor); install elevator regulation device to allow access to top floor only with a special key issuable only to the forms located security, and maintenance staff.

Security manager needs to set in motion a formidable security and crime prevention programme. It will be his job to monitor the results of his efforts. If they are found to be satisfactory, he will look to improve on the efficiency of those measures, and if they have proven to be total failures, he will re-tool his programme with stiffer measures. This part of the job is sometimes overlooked because many consider the job finished and behind them, but really the tasks is just beginning. In short, what management does after the crime prevention programme is implemented will show their level of commitment.

ii. Transportation

Parking Lots/Garages: In big cities and urban centres, one of the most common properties one will use is the parking facility as they are attached to most other properties and may also be independent entities serving a number of properties. Because parking facilities are found in all communities, and are used extensively, and by their very nature contain the means of rapid transportation, they can be the sites of many types of criminal activity. When managed appropriately with crime analysis and prevention considered, parking facilities are secure places for consumers and citizens.

iii. Parking Garage

a) ***Threats:*** Theft from cars

Solution: Install wire mesh from the top of the four-foot walls to the ceiling. This bars quick

access from the grassy area outside the garage while maintaining visibility - thereby avoiding other problems.

b) ***Threats:*** Traffic congestion
Solution: Redirect traffic into one-way flow by closing off multiple exits and entrances. There will be only one way in or out in order to force cars to follow certain patterns that block various escape routes and prevent dangerous crossovers by traffic travelling in different directions.

c) ***Threats:*** Poor surveillance on third level
Solution: Direct traffic toward either one up ramp or one down ramp between the second and third floors. Thereby, all traffic exiting the garage from the second level must pass through the third, creating a deterrent.

d) ***Threats:*** Violent crimes (robbery and rape) in stairwells
Solution: Remove cement stair enclosures and replace with glass walls, increasing visibility and allowing light from other parts of the garage to filter into otherwise darker spaces.

e) ***Threats:*** Auto theft
Solution: Install card-reading access gates at entrances and exits and issue building parking stickers. Post signs reading, "Any car not marked with temporary access tags or permanent tenant tags will be towed at vehicle owner's expense". Follow through on towing to the extent that it does not hurt tenants and their employees.

f) ***Threats:*** Poor natural surveillance from parking garage to building front entrance.
Solution: Cut down the shrubs to a height not to exceeding three feet and remove trees that impede visibility.

g) ***Threats:*** Improve visibility/ surveillance
Solution*:* Move smoker's area from the side of the building to a spot adjacent to the main building entrance, which will enable smokers to see and be seen from parking garage.

h) ***Threats:*** Poor visibility
Solution: Install lighting, especially on the second level, which is devoid of the natural light dispensed to the more open ground and third levels.

i) ***Threats:*** Violent crimes/emotional well-being
Solution: Upon request, provide employees and clients with escorts to their vehicles.

Visualising an improved environment and satisfied with his preliminary changes to the way the parking garage will operate and appear, our manager turns his attention to the security of the building property.

iv. Banking Halls
Banks and Automated Teller Machines (ATMs): Banks have been robbery targets as long as they have been in existence. With bank management comes specific crime prevention standards, and most bank managers are well versed with these standards. The primary focus here is more on crimes occurring in the banking premises and at ATMs, where quick cash is the prime target for criminals.

The Nigerian banking industry has recognised the threat that banking industries and ATM machines pose to the banking public. In effect, customers are often locked out of the safety of the bank lobby and, therefore, totally subjected to die, security preparations or lack thereof, dictated by bank management. Additionally, the banking public is lulled into a false sense of security when utilising ATMs. After all, banks often go out of their way to exude a sense of stability, confidence, and security in the bank lobby. Bank personnels appear attentive; there are often video cameras, electronic devices, telephones, alarms, alert security officers, vaults, safety glass, and two-way windows; and tellers are behind tall counters that instil stately confidence on the part of customers. There is also the message - Your money is secure and so are you!

To further illustrate the general banking industry understanding of the dangers posed to ATM customers, include alarm systems,

surveillance cameras, secure enclosures, and ATM crime prevention education programmes for customers.

The banking industry has known for years that ATM crime is a growing problem. The following recommendations was contributed by industry experts to improve customer safety while utilising ATM devices:

1) Determining the crime risk in the geographical surroundings;
2) Locating new ATMs in highly visible areas;
3) Providing sufficient lighting at and around the ATMs;
4) Educating customers periodically by mailing a notice advising of risks associated with using the ATM and how to avoid these risks;
5) Maintaining shrubbery and other environmental features at a height at which they cannot be used for concealment;
6) Conducting and documenting periodic security surveys at the ATM;
7) Providing a direct-line phone to law enforcement or bank security so that customers can call for assistance around the clock; and
8) Educating bank personnel to be responsive and sensitive to customer claims and to communicate such claims immediately to bank security (Marshall and Pylitt, 1987).

ATM crimes have become a nationwide dilemma that customers and bank operators must face. Security deficiencies at banks can play a critical, contributory role in attacks *on* customers and are of paramount importance when considering vulnerabilities and causation in civil litigation. The ATM was never intended as a replacement for the safety and security of the banking lobby.

a) ***Strip Centres and shopping malls:*** Malls and shopping centres often confront similar concerns as retail stores on a grander scale as they occupy more space, more people visit, and there is more merchandise. Shopping centres are essentially collections of retail stores and other properties in a large building or group of buildings that share common areas such as parking lots and storage areas. Strip centres with many restaurants, bars, and nightclubs may require more security measures than their retail only counterparts.

Because many shopping centres benefit financially from high-traffic locations, and open and inviting layouts, management should take full advantage of crime analysis and prevention. Beyond the scale, the shared common areas set shopping centres and malls apart from stand alone retail stores. Centres management is concerned with security of the entire complex, including the parking lot, sidewalks, and other common areas, not simply a store's internal areas. Even though shopping centres conceivably have more targets than stand-alone retail stores, they possess an advantage in that the cost for implementing crime analysis and prevention measures may be shared by all tenants. Despite access control difficulties, the high traffic in parking areas creates an advantage in its inherent deterrence effect.

Shopping malls are also able to share crime prevention costs with all tenants, though they contend with different dynamics altogether as they are closed in and often isolated from neighbouring properties. Their large size and non-standard configurations make surveying, patrolling, and securing the property a formidable task. Most major malls employ in-house security personnel for the myriad common areas, multiple entrances, and not serve as customer service and information officers.

b) ***Convenience Stores:*** There is not an area of the country or any neighbourhood that does not include at least one convenience store, from the finest neighbourhoods to those plagued by numerous violent crimes on a daily basis. Though technically classified as stand-alone retail stores, convenience stores often deal with more challenges than other retailers. Unlike any retail store whose target consumer can be quite specific, convenience stores strive to meet the smaller, universal needs of just about every consumer at some point in time. Predominantly a cash-based business and one

that is open late hours; convenience stores face threat daily that range from shoplifting to armed robbery, and all too often, murder.

Common deterrence measures include a central cash register location, CCTV, unimpeded views out of the store, limited signage in windows, proper lighting, drop safes, and of course, proper employee training. Policies and procedures should include:

1. Acknowledging customers upon entrance, which serves as quality customer service and discourages criminal activity by putting a face to the crime.
2. Completing merchandise stocking and trash disposal duties before the night shift begins in order to be in a position to view the store at higher risk times.
3. Locking doors at nightfall and operating via a window service.
4. Keeping emergency numbers accessible.
5. Building rapport with uniform police officers working in the area.
6. Posting signs while not obscuring sight lines into and out of the store.
7. Being cognisant of and reporting acts of crime or suspicious activity to police, and recording the same for management purposes.
8. Making frequent bank deposits to reduce the amount of cash in the store.
9. Requesting payment in advance for gasoline to avoid the additional concern of criminals driving off after pumping gas.

8.0 SECURITY DESIGN AND INTEGRATION FOR CRIME PREVENTION IN RESIDENTIAL AND COMMERCIAL ENVIRONMENT

Critical assets can offer extremely attractive targets for a variety of threats. Threats can range from unsophisticated activist groups to highly sophisticated. well-armed and trained professional career criminals or narco-terrorists. While the nature of the threat is key to security design and integration effort, in many cases the consequences of loss for a small or medium firm due to even a medium-level threat can be catastrophic when a key business asset has been compromised.

Some security organisations place undue emphasis upon the selection and application of security personnel or equipment alone without equal consideration of the full range of options and countermeasures that comprise a totally integrated security system. Security managers must avoid the tendency to emphasise a single solution or approach and they must strive to achieve a virtually seamless mix of security countermeasures designed specifically to address anticipated threats and risks. More important, soaring human power and equipment costs coupled with the risk posed by the ominous insider threat demand the effective application of state-of-the-art security countermeasures at key locations to reduce asset vulnerability and keep operational costs under control.

The Security Design and Integration process applies equally to the security manager as system user and the architect/engineer as system designer. This approach will ensure the proper selection and combination of human power, procedures, information, facilities, and equipment into a fully responsive and operationally effective system at a reasonable cost.

System Objectives

Security system is an integrated combination of barriers, technologies, personnel, and procedures designed to safeguard personnel, property, and operations. System objectives generally address deterrence, denial, detection, delay, assessment, and response options based upon a precise definition of threat and user requirements.

It is essential that the security manager recognise that complete systems incorporate a wide range of measures to achieve stated objectives. In the case of a fully integrated security system, protection objectives are achieved through the selection and integration of protective measures from the following range of subsystem options:

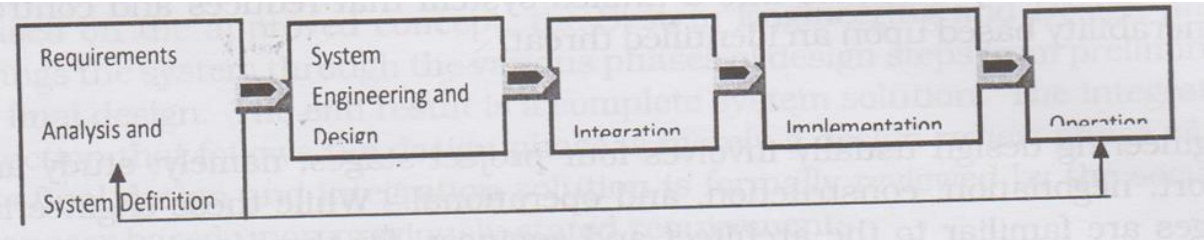
a) Facilities, architectural barriers, and space definition to deter and delay the movements of an adversary.
b) Physical system equipment designed to detect, assess, and in some cases,

respond to intrusion attempts and unauthorised activities.

c) Communications and control and display networks to collect, integrate, transmit, and display alarm and other data for operator response and to control activities of the response force.

d) Security personnel to conduct day-to-day security programme operations, management and system support, and response to non-routine events.

e) Security procedures to guide security operations and provide overall security programme direction and control.



The Design and Integration Process

The essence of design is to invent an order or arrangement of components and details of a system in accordance with a plan. In all cases, whether for security or any other function, a system is designed for a purpose. In the case of security design, the plan is to select and incorporate the various physical elements, personnel, and procedures into a unified system that reduces and controls vulnerability based upon an identified threat.

Engineering design usually involves four project stages, namely: study and report, negotiation, construction, and operational. While these engineering stages are familiar to the architect and engineer, for the security manager, some adjustments are necessary in order to arrive at a process that includes not only the functions of engineering design, but also the integration of tangible and intangible elements resulting in a responsive protection system design.

The essence of integration is to make a whole by bringing together individual parts. For the security manager, system integration is the art of fusing security equipment, facilities, personnel, and procedures together seamlessly in a manner that produces pro-active asset protection.

The end result is a fully integrated security system that responds effectively to dynamic threats and risks during crisis conditions and, at the same time, functions imperceptibly during normal conditions.

Whereas design results in the various security elements responding to a threat or risk, integration fuses them into a workable, day-to-day strategy for effective asset protection.

Security system design and integration begins with a thorough requirement analysis and concept definition. Facility and site protection plans are always based on the identification of critical assets requiring protection and the identification of appropriate countermeasures for each asset. Barriers, electronic hardware, personnel, and procedures are selected to interplay at key locations within the design scheme to form an integrated subsystem protection scheme.

The system concept is formed through the collection of integrated approaches at each asset, facility, and group of facilities sharing a common boundary. Given the diverse missions found in organisations, the integration of protective measures and resources does not involve a static set of environments. Because threat is normally dynamic at each asset or facility requiring protection, the fully integrated system concept must allow for various scenarios, system redundancy based on criticality and collective management of available resources in order to achieve the best possible protective design solution. The security manager is always the final authority

on system options based on requirements stated early in the process and resource constraints.

9.0 A LAYERED APPROACH TO SOLUTIONS TO RESIDENTIAL AND COMMERCIAL SECURITY CHALLENGES

Effective security for residential and commercial property should include a series of layers intended to do the following:

- Create a culture of safety for employees and visitors by providing a high level of accountability and responsibility.
- Prevent and/or mitigate losses by identifying threats before any problems occur.
- Build upon each other to create an integrated strategic response system which is greater than the sum of its parts.

A comprehensive security plan for your commercial property should have at least three layers.

The key to effective security is to make it as difficult as possible for thieves and vandals to cause harm on your property by creating a highly visible outer layer that includes:

- **Fencing:** Secure the perimeter to ensure access is controlled, and that there is no after-hours vehicle access. Fences should be sturdy, at least six feet high and secured at the bottom to prevent anyone from slipping under them. In addition to traditional fencing, other barriers such as artistic bollards or landscaping features present a pleasant visual appearance while also limiting access.

- **Access Control**: Control access to the property by using entry managers and employee ID badges, managing access to both buildings and parking lots where possible.

- **Signage:** Letting people know that they are being monitored is an effective and cost-effective deterrent. Signs should be clean and bright, indicating that security is a priority not an afterthought. Dirty, dented, poorly maintained signs send the wrong message. Signs should also be well lit.

- **Lighting:** Illuminate remote areas such as stairwells and side entrances to ensure the safety of people using them and to deter intruders. This will also enhance your security team's ability to actually see suspicious activity. Even basic steps such as bright lighting and stripes of reflective paint in the parking lot and access areas can improve security in small lots, reports.

- **Photoelectric Sensor Beams:** Photoelectric sensors transmit beams of light that move from transmitters to receivers, which are arranged around the perimeter of your property. When an intruder walks through the beam, they block the transmission to the receiver thereby triggering an alarm. These systems are especially useful for warehouses and auto dealerships, or other storage areas for valuables on commercial properties.

- **License Plate Recognition (LPR):** License plate recognition tracks vehicles when they enter and exit properties. As a component of access control, unapproved vehicles can be denied entry. This system can also be used during investigations of unauthorised investigations to improve incident response.

Layer 2: Inside the Perimeter

The next layer monitors and reinforces the outer layer, using technology that serves as the eyes and ears of residential and commercial property's security system. This security layer quickly responds to threats by using:

- **Alarms**: Leverage audible alarms and silent alarms, linked to a comprehensive system of strategically placed sensors, and actively monitor them to ensure rapid response to unauthorised intrusion. Emergency exit door sensors should be connected to alarms so that a siren is triggered in the event of an emergency evacuation, or if the door is propped open to allow for access later.
- **Guards**: Dedicated security personnel can ensure an immediate response while waiting for local law enforcement who might

have other priorities. Trained to handle best-to-worst case scenarios, security guards patrol and monitor your property, provide assistance to visitors in need and investigate suspicious activity. They also serve as a liaison between your business and the law enforcement community.

- **Surveillance Cameras**: Camera technology has become very advanced and diverse, with different functionality and form factors available to meet specific surveillance needs. Use different types of cameras to fit each situation, such as wide-angle lens cameras focused on storefronts to monitor and deter etching, vandalism and unwanted gatherings. Cameras should be leveraged to monitor activity, especially at loading docks, front doors, lobbies and other entry points. Covert cameras are recommended to combat internal shrinkage in properties like warehouses.

- **Radar-Guided Cameras**: Radar surveillance technology detects intrusions and wirelessly directs connected cameras to point at the intrusion. The system is smart enough to distinguish between real intrusions and other movements that may set off false alarms, ensuring something like tree branches blowing in the wind will not trigger an emergency response. Radar-guided cameras are a cost-effective option due to their long range and versatility, with one mobile camera covering the same ground as several fixed cameras.

- **Drones**: The mobility and interactivity of drones make them a versatile component of any security plan, particularly because they can be fully autonomous, self-charging and deployed 24x7. Furthermore, they require no installation and have low operational costs, especially considering the large areas that they can cover.

- **Mobile Surveillance Units**: Mobile Surveillance Units are a highly visible deterrent that can be moved around based on changing business needs, such as a special event or project. They work particularly well in high-crime areas and for focusing on emergent problems like dumping or vandalism. Supplement the units by pairing them with lights, two-way audio communication and license plate recognition cameras to both deter and document the activities of thieves, as well as to track vehicles and block unwelcome parties from entering.

- **Virtual Guard Services**: ECAMSECURE's Virtual Guard security services combine traditional video surveillance, two-way audio and meticulous guard protocol to deliver a cost-effective and optimised remote system. Virtual guards can perform remote patrol, assist with access control, serve as virtual escorts to staff and visitors on your property and provide alarm verification, in addition to several other duties – at a fraction the cost of an on-site guard.

Wired cameras are highly visible and can provide higher resolution and clearer images than wireless cameras, which is especially useful for forensic analysis.

Wireless cameras are concealable and can be installed in a wider range of locations than wired cameras. They are ideal for covert surveillance.

Network/IP-connected cameras can be wired or connected wirelessly, and can stream footage over the Internet via cables, Wi-Fi, or cellular air cards. They can also be equipped with one-way and two-way audio.

Wide-angle lens cameras can cover angles of up to 104 degrees within a range of about 40 feet. Perfect for larger outdoor areas such as a parking lot.

Pan-Tilt-Zoom (PTZ) camera scan aim, zoom and tilt to 180degrees and reposition to 360degrees in in a split second, capturing minute details like facial features and license plate numbers. They are ideal for larger areas.

Fixed box cameras offer a fixed-angle view and function as an effective deterrent because offenders can see exactly where they are pointing. Ideal for retail locations, warehouses and auto

Bullet cameras are designed to point in a single direction and are well-suited for covering narrow locations like alleyways.

Dome cameras are highly visible and capture a range of angles. They are well-suited for fixed positions such as entryways.

Mobile surveillance units can be set up anywhere on a temporary or long-term basis. They can record surveillance footage locally or stream it to a central location or mobile devices.

Thermal and night vision cameras capture images in dim-light conditions. They are ideal for monitoring auto dealerships sites at night.

Radar-guided cameras offer 360° perimeter security, high-definition video and are designed for both day and night use. They are suited for high-security areas.

Layer 3: Proactive and Effective Monitoring with Rapid Response

The final layer integrates high-tech monitoring capabilities into security design plan, taking it to the next level with:

- **Proactive Monitoring:** Maintain effective surveillance coverage, along with dedicated virtual guards and video verification to ensure full-time monitoring, incident response and reporting.

Video analytics ensure that virtual guards are immediately alerted to any issues, which they can then verify and address as soon as possible. In case of an intrusion, the guard can work to ensure that unauthorised persons leave the property using pre-recorded messaging, two-way audio communication, strobe lights or siren. They can then summon on-site security personnel or local law enforcement, ensuring that they arrive in a timely manner, and interacting with them to resolve the problem in real-time.

Fortify this layer by adding:

- **Thermal Imaging**: Track intruders via their heat signature, without responding to false alarms such as those triggered by animals on the premises using thermal imaging. This technology is also useful for detecting fires and potential overheating of equipment or buildings.

- **ECAMSECURE Smart View:** Smart View is a video intrusion detection system that

is monitored for immediate video verification of an alarm or alert, resulting in a priority police response to the verified security issue.

- **Advanced Analytics:** Detect intrusions and other security threats in real-time by using analytics software, including audio analytics and predictive video analytics to capture signs of break-in, violence or aggression and other problems. Facial recognition software can be used to alert your security team to the presence of a known offender or disgruntled former employee before they cause any harm and allow your team to take an effective proactive approach.

10.0 CONCLUSION AND RECOMMENDATIONS

In every society, one of the implications of poor crime abatement measures is the flagrant abuse of human rights especially the scale of fatalities. This paper has been able to establish the trends and patterns of crime incidents and fatalities by analysing crime reports in Trent Online and Nigeria Watch. While residential and commercial communities in Abia, Lagos, Edo, Delta, Imo and Ogun, located in the Southern zone of Nigeria recorded high incidents and fatalities in criminal activities (armed robbers, cultism and domestic violence), there were few crime incidents and fatalities in the North. Furthermore, Abia State was the most hit by fatal kidnapping, Lagos and Rivers recorded huge fatalities in cultism and armed robbery. To curb crime in Nigeria, it remains imperative to apply the principles of non-killing theory by state and non-state actors into fight against crime from a concerted and multi-dimensional approach.

The challenges of insecurity and criminality in any area often constitute a threat to property and lives thereby hampering daily operations. This is because where individuals especially at work get emotionally traumatised through insecurity at home; there will be a reduction in work efficiency, with a resultant effect on country or states' growths. It is therefore important for government to retrace their steps and formulate a proficient, implementable polices and programme in tackling the root causes of insecurity across states of Nigeria. This can enhance compliment private sector's effort towards home security across the states of the federation. There should also be a supply of stable electricity supply, good road networks and community security systems, to scare away criminals. Unemployment and abject poverty among citizens should be addressed by agencies concerned to aid the reduction of violence and crime in Nigeria. Effective residents and landlord association should also be strengthened with youth being represented to aid security effectives and scare away unwanted strangers. Conclusively, Home security system across Akure, Ondo State Nigeria seems unacceptable to the existing standard in other countries. Hence, there is still need for further actions to improve residential housing security when residents are home or away. Therefore, government at local, state and national level should embark on trainings relating to contemporary systems of intelligence gathering and sharing, logistics and organising of advanced machinery to manage security activities. Youth should mostly be involved in this program as part of solution to unemployment. Safety managements in higher institutions curriculum should also be encourage by government so as to help the youth to advance in the awareness of effective security systems and appreciate the relevance of security in a country like Nigeria. This will curb the incessant crime and mortality rate in the country while values will remain intact.

REFERENCES

Achumba, I. C., Ighomereho, O. S., and Akpan-Robaro, M. O. M. (2013). Security Challenges in Nigeria and the Implications for Business Activities and Sustainable Development. Journal of Economics and Sustainable Development, 4(2), 79-99.

Adegoke, O. J. (2014). "Critical factors determining rental value of residential property in Ibadan metropolis, Nigeria", Property Management, Vol. 32 Issue: 3, pp.224-240.

Ajibola, M. O, Oloke, O. C and Ogungbemi, A. O. (2011). Impacts of Gated Communities on Residential Property Values: A Comparison of Onipetesi Estate and its

Neighbourhoods in Ikeja, Lagos State, Nigeria, Journal of Sustainable Development, Vol. 4, No. 2.

Azid, S. I. and Kumar, S. (2011). Analysis and Performance of a Low Cost SMS Based Home Security System, International Journal of Smart Home, Vol. 5 No. 3.

Azuh, M. (2012). Safeguard your Home with Affordable Security System. Published in Punch Newspaper February 21st.

Abolurin, A. (2010). *Crime Control in Nigeria, 1999-2010*. Ibadan: John Archers Publishers Ltd.

Brunson, L., Kuo, F. E. and Sullivan, W. C. (2001). Resident Appropriation of Defensible Space in Public Housing Implications for Safety and Community, Environment and Behavior, Vol. 33 No. 5.

Budijono, S., Andrianto, J. and Novradin, M. A. (2014). Design and Implementation of Modular Home Security System with Short Messaging System, EPJ Web of Conferences.

De Biasi, A. (2017). Transforming Vacant Lots; Investigating an Alternative Approach to Reducing Fear of Crime, Journal of Environmental Psychology 50, pp. 125-137.

Downing, I. (2007). Centralized Integrated Security Optimal for Residential Estate. i to i Technology, South Africa, Internet.

Hannah, G. (2011). Professional Home Security Monitoring. Internet.

Johnson, T., Davis, K. and Shapiro, E. (2000). Modern Methods of Valuation of Land, Houses and Buildings. Estate Gazette, London, pp. 295-340.

Khanna, S. V. and Omprakash, (2011). Wireless Home Security System with Mobile, International Journal of Advanced Engineering Technology, Vol. II No IV pp.396-397.

W. e. n. d. y. L, Sage-Jacobsen, S. and Webb, E. (2016), Single Ageing Women and Housing Security: A Pilot Project in the Cities of Unley and Salisbury.

Newman, O. (1996). Creating Defensible Space. Washington, DC: U.S. Department of Housing and Urban Development, Office of Policy Development and Research.

Newman, Oscar (1978). Defensible Space. Crime Prevention through Urban Design. Macmillan, New York.

Okonkwo, R. I., Ndubuisi-Okolo, P. and Anagbogu, T. (2015), Security Challenges and the Implications for Business Activities in Nigeria: A Critical Review, Journal of Policy and Development Studies Vol. 9, No. 2,

Newman, O. (1972). Defensible Space: People and Design in the Violent City. London: Architectural Press.

Olabanji, O. E., Ese, U. (2014). Insecurity and Socio-Economic Development in Nigeria. Journal of Sustainable Development Studies ISSN 2201-4268 Volume 5, Number 1, 2014, 40-63.

Olaniran, M. O. (2006). Nation-Wide Property Identification and Land Registration as Basis for Sustainable Reform, Growth and Safety. ENVIRON-LINK Journal Vol.1 No2, School of Environmental Studies, Federal Polytechnic Ado-Ekiti, Ekiti State, pp 114.

Olajide S. E. and Bello, I. K. (2003). Element of Property Valuation. Campus Publication Ltd., Lagos. pp. 87-90.

Olajide, S. E. (2010) Critique of Residential Property Values in a developing Economy. Lecture mimeograph on Advanced Valuation. Fed. Poly Ado. pp. 7.

Olajide, S. E, and Kolawole, A. O. (2013). Security Challenges in Nigerian Residential Real Estates. Journal of Environmental Science, Toxicology and Food Technology (IOSR-JESTFT) Vol. 2, Issue 5, PP 08-14

Olajide, S. E. and Mohd Lizam, M. D. (2017). Appraisal of security challenges within the Nigerian Residential Neighbourhood; In search for a sustainable theoretical framework, The Soc. Sci, 12 (3), 517-523.

Onifade, F. A. (2007). Estate Security. Unpublished Lecture notes on Property Management. The Federal Polytechnic, Ilaro, Ogun State, Nigeria.

Radetskiy, E. L., Spahr, R. W. and Sunderman, M. A. (2015). Gated Community Premiums and Amenity Differentials in Residential Subdivisions.

Seldon, Andrew (2007). Home Security Challenges. Internet. www.homesecuritystore.com Pp1959

Soares, R. (2009). "Welfare Cost of Crime and Common Violence: A Critical Review." The Cost of Violence. Washington DC, United States: World Bank

Olukayode Durojaiye T.O.L. Planning and Management of Cities and Rural Areas in Nigeria for Sustainable Development: Security and Safety issues.

Chapin, F. S. (1970). *Urban Land* Use Planning. University of Illinois Press, Chicago.

COHRE (2006). *Forced Evictions:* Violations *of* Human Rights, Global Survey No 10, COHRE, Geneva.

Durojaiye, O. (2008). *The* Millennium *Development* Goals and *Poverty* Reduction in *Nigeria.* Paper presented at the 3rd National Conference of Urban and Regional Planning Department, Yaba College of Technology, Yaba, Lagos.

Keeble, L. (1961). *Principles* and *Practice of Town* and Country Planning. Estate Gazetter Ltd. London, pg. 9

Morka, F. C. (2007).`*A* Place *to Live.* A Case Study *of the joraHadiya* Community, Lagos, *Nigeria',* unpublished case study prepared for Global Report on Human Settlements, 2007.

Nwaka, G. I. (2005). *The Urban* Informal *Sector in Nigeria: Towards Economic* Development, Environmental Health, and Social *Harmony'.* Global Urban Development Magazine, Vol. 1.

Okude S. A., Ademiluyi I. A. (2006). Coastal *Erosion In Nigeria: Causes, Control and* Implications. International Digital Organisation for Scientific Information. Vol. l, No. 1:44-51.

UNDP (2003). Human *Development Report 2003:* Millennium *Development* Goals: *A Contract* among Nations *to End* Human *Poverty.* New York: Oxford University Press, for the United Nations Development Programme.

UN-Habitat (2007). Enhancing Urban Safety and Security: Global Report on Human Settlements, Earthscan, London.

USAID (2002). Making Cities *Work: Urban Profile of Nigeria.*

Adalemo, Isaac Ayinde (2003). Security and Safety: Panacea for the Enhancement of Democracy and National Development.

Agboola, T. (1997). The Architecture of Fear: Urban Design and Construction Response to Urban Violence in Lagos, IbadanIFRA/African Book Builders.

Akowonjo, Dipo (2004). Security Systems: Conceptual Foundations, Structure and Development.

Alexander, C., Ishikawa, S., Silverstein, M. (1977). A Pattern language: Towns, Buildings Construction. New York-Oxford University Press.

Brundson, C., Gilroy, R. *et al* (1995). Safety. Crime, Vulnerability and Design - A Proposed Agenda of Study. New Castle Upon Tyne. Environment and Safety Group. Corbett, J. (1985): Alice Coleman: Design Disadvantagement. http: / /www. csiss. ora/classics/content/41

Cozen, P. (2004). Urban Sustainability and Crime prevention Through Environmental Design (CPTED) in Western Australia (175th Anniversary State Conference - A shared Journey).

Cozens, P., Hillier, D., and Prescott, G. (2001). Crime and the Design of Residential property - Exploring Perceptions of Planning Professionals, Burglars and other Users. Property management. 19: 4, 222-248. MCB University Press.

Garland, C. A. and Stokols, D. (2002). The Effect of Neighbourhood Reputation on Fear of Crime and Inner-City Investments. In Aragones, J. I. Francescato, G. & Garling, T. (eds.) (2002). Residential Environment - Satisfaction and Behaviour.

Gifford, R. (1997). Environmental Psychology - Principles and Practice. Allyn and bacon Pub. Boston.

Hill, J. D. (2002). Crime Prevention through Environmental Design and Community Policing. Sheriffs Office. http: /www.clea.org/newweb/newsletter/No.79/crimeprevention.h tml.

Broder, J.F. Risk Analysis and the Security Services. 2nd Edition.

Matka, E. (1997). Public Housing and Crime in Sydney. NSW Bureau of Crime Statistics and Research.

Moran, R. and Dulphin, G. (1986). The Defensible Space Concept - Theoretical and Operational Explication. Journal of Environment and Behaviour. 18: 3, 396-416, Sagie.

Newman, O. (1972). Defensible Space. Macmillan. New York.

Newman, O. (1996). Creating Defensible Space. New York, Office of Policy Development and Research (HUD).

Okunola, S., and Amole, D. (2006). "Key Factors in Crime and Sustainable Housing Development.

Poyner, B. and Webb, B. (1991). Crime Free Housing. Butterworth, London.

SECURITY PERCEPTION COMMUNICATION AND POLITICS

COMMUNICATION IN MANAGING SECURITY CHALLENGES IN NIGERIA: REFLECTING ON WAY FORWARD

Adebayo Akinade dfisn

ABSTRACT

This paper examines the various security challenges facing Nigeria, including insurgency, secessionist movements, and militancy in the Niger Delta region. It also analyzes the role of communication, both traditional and digital, in addressing these challenges and promoting national security. The study highlights factors contributing to security threats, such as inadequate technological infrastructure, unemployment, poverty, and poor governance. Recommendations include the procurement of advanced technological systems, proactive government welfare policies, strategic communication strategies, collaboration among security agencies, and efforts to foster national development. Overall, the paper emphasizes the importance of effective communication and collaboration in addressing Nigeria's security challenges and promoting peace and stability.

Security of a State refers to the ability to itself profile from external dangers and menaces which includes intervention, blockages, invasion, destruction occupation or harmful interference by hostile groups from powers or terrorists. The method of State security is to deter prevent or defend attacks against the state goal and its security science is an idea that brings together many concepts and principles.

It is important that security science develops a structured and defined body knowledge with a clear context or practice and principles and guidelines security science is an emerging academic that brings discipline together into body concepts of knowledge.

The paper will examine the science and technological issues in security and the effects on the productivity and the extent of its motivation on security personnel and the citizens protection. The paper will look into innovation management of security science and technology development.

This paper deals with the roles of communication in security challenges which is dynamic and multi discipline. The security practitioners need to keep abreast with current and recent trends and issues in security challenges and communication issues. These aspects of communication keep the security profession to be current.

The paper focus on roles of communication in resolving security intelligence because the world has moved beyond mere gathering challenges of information but analyse them and keep them for the practice.

The paper will enhance the standard of security practice. The paper also covers the following areas:

- *Concepts and the Roles of Communication in Dealing with Security Challenges*
- *Elements of Security and Communication.*
- *Security and Communication Skills.*
- *Application of Principles/Practices of Communication and Security*
- *Communication and Security: Practices and Techniques*

The paper is primarily designed for security practitioners and personnel. Security communication involve normative and appreciates the challenges involved. The paper suggests solutions to the problems.

Keywords Communication Challenges, Security Challenges, National Security, Communication And Digital Age

INTRODUCTION

The security of any nation can be enhanced or truncated by communication channels; interpersonal relations, the traditional media, social media as well as others including music. Strategic communication enables and supports other aspects of national security in terms of policy planning and implementation.

With the evolving communication patterns and technology such as social media, the government in conjunction with the traditional media also needs to evolve and adopt strategies that strengthen and safeguard the nation on both online and offline platforms without trumping individual liberties and privacy. Nigeria must realize the efficacy of communication as a tool in solving internal and external threats to national security and use it to its advantage in ensuring peace and stability within its borders and in its interaction with foreign counterparts.

A crisis which is a result of security challenges, secession and insurgent attacks is seen in most parts of the world including Nigeria, as something abnormal, dysfunctional and detestable. They are generally described or regarded as enemies of peace and development. Yet, it is a fact of life and can be a precursor of positive change because no condition is permanent. Likewise, Corruption, impunity, molestation of citizens, marginalization, and militias on oil and gas facilities in the Niger- Delta has added to compound the unpalatable consequences of Boko Haram, cases of unknown gunmen, conventional crimes, kidnappings, killings, trafficking, and domestic violence across all regions of the country. Adeniyi (2016) avers that "looters ruled Nigeria for years, politicians became rich, corporate houses became richer and masses in Nigeria remain in abject poverty and hunger. Essentially, effective crisis management handles these threats sequentially with the use of communication processes, techniques and media to enable citizens to be abreast of the situations within and around them in society.
The necessity for effective and regular communication from the government to the citizens is built on the understanding that an effective democracy is one where the citizens are aware of government activities because an informed populace is a more effective partner to government developmental efforts without which good governance may be more difficult to achieve (Fairbanks, Plowman, & Rawlins, 2007).

Regrettably, the government on this bestowed constitutional responsibility has failed to provide a secure and safe environment for lives and properties including the economic activities of the country. Also, one of the major functions of a modern state is the provision of social amenities and employment to the people, coopting them in decision-making and empowering the local communities to reach out to the aggrieved parties or perpetrators of the acts with a message of peace and reconciliation, dialogue and discussion as communication techniques and win-win approach before it escalated to this unimaginable level due to stick and carrot approach. These aspects, however, create a public worry and force the general public to seek help from the most accessible ways available to them. For most people, it's either the internet, social media, or print or broadcast media for information and options for safety.

COMMUNICATION CHALLENGES IN EMERGENCY RESPONSE

A primary challenge in responding to security challenges, natural and man-made disasters is communication. Responding organizations must work in concert to form a cohesive plan of response. However, each group of security community; fire, police, SWAT, HazMat communicates with radios set to orthogonal frequencies, making inter-agency communications extremely difficult. The problem is compounded as more local, state, and federal agencies become involved.

The communication challenges in emergency response go far beyond simple interoperability issues. Practical observation of first responder exercises and drills, and workshop discussions, we have identified three categories of communication challenges: technological, sociological, and organizational. These three major areas are key to developing and maintaining healthy and effective disaster communication systems.

The primary technological challenge after a disaster is rapid deployment of communication systems for first responders and disaster management workers. This is

true regardless of whether the communications network has been completely destroyed (power, telephone, and/or network connectivity infrastructure), or, as in the case of some remote geographic areas, the infrastructure was previously nonexistent. Deployment of a new system is more complicated in areas where partial communication infrastructures remain, than where no prior communication networks existed. This can be due to several factors including interference from existing partial communication networks and the dependency of people on their prior systems.

Another important obstacle to overcome is the multi-organizational radio interoperability issue. To make future communication systems capable of withstanding large- or medium scale disasters, two technological solutions can be incorporated into the design: dual-use technology and built-in architectural and protocol redundancy.

Dual-use technology would enable both normal and emergency operational modes. During crises, such devices would work in a network-controlled fashion, achieved using software agents within the communication availability, and applicability of emergency communication solutions.

Sharing and dissemination of information is both critical and problematic, beginning with whom to trust in unfamiliar settings. Even after a level of trust is established, security issues must still be considered. Another important factor is the emotional volatility of the victim population. Fear, stress, and other emotions are aggravated by the lack of information. Therefore, periodic information updates are important. Hegde et al. presented a technological solution that provides differentiated services for an agitated caller by detecting the emotional content in speech packets over a wireless network.

Some technologies created to improve communications among and across responders and their many agencies may not be willingly adopted. This can be due to several factors, some of which involve resource constraints that inhibit the purchasing or upgrading of equipment and paying for training costs (which can be prohibitive) to learn new technologies not used on a regular basis.

At a higher level, the lack of a common vocabulary between response organizations and between organizations and citizens adds to the problems. While the communication between organizations has improved in terms of a common language, it still lacks efficiency. Additional social science research is needed to investigate common languages and principles such as icon languages for use between response organizations and the victim population. Above all, the emergency communication tools for the general public must be affordable, available, and applicable during their day-to-day life in order to ensure that they will be used during a crisis.

Organizational challenges are prevalent in disaster response, especially when groups that are accustomed to hierarchy and hierarchical (centralized) decision making must suddenly work in a flatter, more dynamic, ad-hoc organization that emerges during post-disaster relief efforts. There are advantages to both. Collaborative technologies such as mobile applications, Web-based email, and communications applications such as Groove can aid in the effectiveness of cross-organizational communication. Hierarchical organization leads to wider information gaps across organizations, but flat organizations are not scalable. Therefore, a hybrid organizational model needs to be developed to best utilize the two organizational approaches. The availability of information has a temporal dimension. For example, there is a significant lack of information about the scale of a disaster in the immediate aftermath; this is followed by large amounts of imprecise information. The chief challenge for the emergency response organization is not the scarcity of information, but the glut: too many resources and too much information strains the capacity of the management system as well as the communication system. Art Botterell observed that while communication failures tend to propagate downward (begin with

culture, but ultimately blame the technology for failing), the change needed to address these failures must propagate upward: given an enabling technology, new procedures for use are required, human and organizational factors must be considered, and ultimately the entire culture of an organization may need to be changed.

In conclusion, only a comprehensive approach involving solutions for each of the three major issues technological, sociological, and organizational can provide a reliable communication system during crisis situations.

Security challenges

Presently, no state in Nigeria is not disturbed or faced with one form of insecurity or the other and this has constituted a serious threat to public safety and national security. According to the revisionist cited in Okoli, (2012), national security means freedom from all forms of social, socio-economic, ecological, territorial, economic and socio-political vulnerabilities. Security embraces all measures designed to protect and safeguard the citizenry and the resources of individuals, groups, businesses and the nation against sabotage or violent occurrences (Ogunleye, et al, 2011). Some scholars conceptualized security as emphasizing the absence of threats to the peace, stability, national cohesion, and political and socio-economic objectives of a country (Igbuzor, 2011; Oche, 2001). In other words, insecurity is the state of being exposed to threats, risk or anxiety. Nigeria the giant of Africa is faced with numerous challenges due to Boko-Haram, banditry, Endsars, pandemic, sit-at-home and other security vices.

Security is about encouraging liberal institutions to discharge their responsibilities creditably and also having universal respect for the development of society and upholding human dignity. Persistent ethnic conflicts and religious clashes between the Islamic groups and Christians, political consciousness, claims over resources, a secessionist state in what was then known as eastern Nigeria that caused the Nigerian civil war from 1967-1970 now declaring itself Independent People of Biafra, Sharia and Islamic State and so on present the country with major security challenges.

In the past, there was no law in Nigeria to punish citizens who engaged in acts of terrorism, as a result, in 2011, former president Goodluck Ebele Jonathan enacted the Terrorism Act, and the law was passed and amended in 2013 as the Terrorism Prevention Amendment Act. Despite the law and efforts by the government, security agencies and humanitarian organizations in combating these crimes, attacks are still meted out on citizens daily. According to Section 2656f(d) of Title 22 of the United States Code, Terrorism is the systematic and premeditated use or threatened use of violence for politically motivated purposes, that has been described as the "weapon of the weak." By staging attacks which are unexpected and which intimidate a larger audience than their immediate victims. Small groups of terrorists can influence public opinion and, through this, gain a measure of control over the policies of much larger and militarily stronger nations. Today, terrorist attacks are far larger in scope and innovative in their methods. In 2006, a terrorist group called the Islamic State of Iraq and the Levant (ISIS) meted terror against the people of Turkey in Istanbul airport where scores of dead bodies were gathered. It was also reported by Gul Tuysuiz and Steve Almasy that not less than 36 citizens were feared dead and 147 injured in that particular attack. Baghdad, the capital of Iraq was also visited by its devastating bomb attack that recorded the worst terror where at least 199 citizens were killed (CNN, 2016).

In Nigeria, the research group Armed Conflict Location & Event Data Project cited in The Guardian Newspaper of April 28, 2022 reports that bandit militias killed more than 2,600 civilians in 2021, an increase of over 250 percent from 2019 and 2020. However, the National Assembly in 2011 enacted an Act on terrorism eradication. Accordingly, the Act in section 1 (3) explains the act of terrorism as one which is deliberately done with malice and which involves or causes an attack upon a person's life. Which may cause severe bodily harm or death, kidnapping, destruction of

government or public facilities, seizure of aircraft, ships or other means of public transportation. Others are the manufacture, possession, acquisition, transport, supply or use of weapons, explosives or nuclear, biological or chemical weapons as well as research into and development of biological and chemical weapons without authority; the release of dangerous substances or causing of fire, explosion or floods, the effect of which is to endanger human life; interference with or disruption of the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life and an act or omission in or outside Nigeria which constitutes an offence within the scope of counter-terrorism protocols and convention duly ratified by Nigeria. The federal government had declared that bandits were also terrorists in November 2021, making the activities of Yan Bindiga, Yan Ta'adda and other similar groups illegal. For example, Institute for Security Studies research has shown an increasing nexus between bandits and jihadist groups such as Boko Haram and Ansaru terrorists. These violent extremists are key players in violent crimes and terror activities especially in the north-west and north-central Nigeria.

Insurgency

The insurgency has been defined as an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict (Haviland, 2012). The Counter-Insurgency Initiative (2009) has defined insurgency as the organized use of subversion and violence to seize, nullify, or challenge political control of a region. Insurgents seek to subvert or displace the government and completely or partially control the resources and population of a given territory. They do so through the use of force (including guerrilla warfare, terrorism, coercion or intimidation, propaganda, subversion, and political mobilization). It means individuals or groups rising upon or against destabilizing government authority or development of a country by posing a threat and acting aggressively to other members of the society. Boko Haram which is part of insurgency in Nigeria means "Western education is forbidden" was founded in 2002 in Maiduguri in Northeastern Nigeria by a charismatic Muslim cleric, Ustaz Mohammed Yusuf. The sect's philosophy is rooted in the practice of orthodox Islam, and the group's official name in Arabic, Jama'atu Ahlissunahlidda 'awatiwal Jihad, translates to "people committed to the propagation of the Prophet's teachings and Jihad". Boko Haram is an Islamist movement that is tied to Al-Qaeda and its followers forbid Muslims or its groups to be involved in any political or social activity that is related to Western education or ideology.

It also translates as 'Western education is sin' or ''Western Civilization is forbidden'' (Peters, 2014, p.186). The Islamic sect believes that Nigerian society is so corrupt and ubiquitous, that a devoted Muslim must migrate to a society that is free from deprivation and marginalization. Akanji (2009) observes that the goals of Boko Haram are to overthrow the Nigerian government, incite religious tensions through acts of terror and eventually declare an Islamic state in Nigeria. Similarly, terrorism is defined as the systematic use of violence and intimidation to coerce a government or community into acceding to specific political demands (Pearsall & Trumble, 2006). These sects have carried out several attacks on schools, churches, mosques, banks, military, paramilitary and police formations, media houses, markets, and other strategic places resulting in many deaths and increased media coverage. They insist on the supremacy of the Islamic culture.

From its recent activities, the group can also be said to be anti-Christian going by the rate it has been attacking Christians and bombing churches. Zalman (2014) opined that religious fanaticism creates conditions that are formidable for terrorism. Since 2011 when the insurgents started their large-scale bombings and killings mainly in the North-Eastern part of Nigeria, an estimated number of 15,000-18,000 citizens have been killed (CNN, 2015; Vanguard, 2015). Similarly, The Punch reports that ''Boko Haram has devastated Northeast Nigeria in its quest to create an Islamist state, killing over 20,000 people and displacing 2.6

million from their homes'' (The Punch, 29th October 2016). However, because of the obnoxious styles of banditry activities, banditry is x-rayed in criminal feats such as cattle rustling, kidnapping, armed robbery, drug abuse, arson, rape and the brazen and gruesome massacre of people of agrarian communities with sophisticated weapons by suspected herdsmen and reprisal attacks from surviving victims, a development that has been brought to the front burner of national security (Uche & Iwuamadi, 2018). In his view, Shalangwa (2013) regards banditry as the practice of raiding and attacking victims by members of an armed group, whether or not premeditated, using weapons of offence or defence, especially in semi-organised groups to overpower the victim and obtain loot or achieving some political goals. Such bandits are usually perceived as outlaws, desperate and lawless marauders who do not have a definite residence or destination but roam around the forest and mountains to avoid being identified, detected and arrested by government agencies. They operate within and along rural borders with the assistance of their local collaborators including in some cases, state agents deployed to work for the safety and security of the people (Abdullahi, 2019). Thus, economics, selfishness, corruption, poverty, hunger or political interests, ethnicity, and so on have continued to stimulate insurgency in Nigeria.

Secession

Secession refers to a deliberate voluntary effort to organize individuals who act in concert to achieve group influence and make or block changes. It is not uncommon for groups who have fought and lost a secession war to request for independence. Shared victimhood makes for easy mobilization of support. However, the Igbos continued to feel alienated from Nigeria after the civil war. They believed they had been excluded from the political and socio-economic mainstream of the country, and the clamour for a separate existence from Nigeria continued to gain momentum. This eventually led to the establishment of the Movement for the Actualization of the Sovereign State of Biafra (MASSOB) in 1999. Onwe, 2011, described MASSOB, as a non-violent separatist movement, with its philosophy hinged on the principle of non-violent conflict as propagated by Mahatma Gandhi, was founded by Ralph Uwazuruike, a lawyer, on 13 September 1999. MASSOB advertised a 25-stage plan through which its goal for peaceful secession from Nigeria would be achieved. MASSOB successfully mobilized Igbos in the country to shut down their businesses for a day on 26 August 2004 and embarked on demonstrations in Canada, Germany, Italy, and France. Their activities provoked the government and led to several arrests of Uwazuruike and his followers for unlawful gatherings and the disruption of public peace. In July 2000, Uwazuruike was arrested for storming the 36th Organisation of African Unity (OAU) Summit in Lomé. He was again arrested and arraigned for treason in Abuja in 2005. He was released on bail in 2007 after some political interventions and finally discharged and acquitted with his members in 2011, during the Goodluck Jonathan administration. The movement has since lost steam, as it failed to gather the support of the south-east governors amid concerns in certain quarters that the movement was too politicized.

Another group, the Biafran Zionist Movement (BZM), was founded in 2010 by a United Kingdom-based lawyer, Benjamin Onwuka, who said it was founded to give "seriousness" to the Biafran dream. The group submitted an application to the United Nations (UN) Secretary-General, Ban Ki-Moon for observer status for the Republic of Biafra in 2012. Onwuka's attempt to declare himself as the leader of the new Biafran Republic in a live broadcast resulted in a gun battle with the police, and his members' subsequent arrest. They were charged with treason but granted bail. Onwuka and his members were again arrested in 2018 while marching to Enugu State Government House to hoist the Biafran flag. They are now on trial. However, the agitation of their followers was revived when their next leader, Nnamdi Kanu emerged. It was he who made the defence of IPOB and was so articulate and faithful that the movement towards actualizing it would not be hampered

by any government. The movement according to them was setting aside Igbo people's dependence and subservience, self-determination, unity of Igbo people and the need to be treated with dignity as equals to other people in all parts of the world. According to Onwe, 2011, the movement stresses coexistence based on equality and respect for human dignity, it stands for the political, economic, and cultural unity of Igbo people both at home and in the diaspora. It rejects all forms of non-indigenous control of the whole of the South East, economic and political system.

However, this secessionist due to the arrest and manhandling of their leader, Mazi Nnamdi Kanu by the government brought to force the issue of sit–at–home agitating that the federal government must release their leader. This scenario has been on and citizens around this region always adhere to the order for the safety of their lives. Due to these issues at stake, The Guardian Newspaper, 2021 reports that the Nigerian President was scheduled for an official visit to Imo State on September 9. 2021, but was marred due to poor turnout of Imo residents because they were afraid of attacks due to the sit-at-home order by secessionists to express their grievances over the detention of their leader which often culminate multifaceted security challenges affecting the economy and citizenry of the country.

Niger -Delta Militancy Agitations

Just as the Nigerian military seems to be making way in the Northeast, a new wave of militancy erupted taking over the Niger -Delta region with the notion of a militant group called the Movement for the Emancipation of the Niger- Delta (MEND) to the Niger Delta Avengers (NDA). These incidents in that region of the country attracted international headlines in the early 2000s when the oil-producing region was surrounded by militancy claiming responsibility for the pipeline vandalization and bombing of oil installations in the troubled region, agitating to deal and cripple economic activities in the area if they are not treated fairly by the government. This however brought about a serious battle between this group and the government, including an all-time low of less than $50 per barrel oil production in Nigeria and somehow yielded good fruit to the people in that region due to governments' attention to their quest.

The Ogoni agitations

Ogoni have since the independence of Nigeria, suffered under systematic political marginalization and environmental degradation of their ancestral lands and exploitation of natural resources in tandem with Western energy giants of Nigeria's oil-rich Niger Delta. The Ogoni's peaceful civil resistance movement was organized by the Movement for the Survival of the Ogoni People (MOSOP). In May 1994, nine activists from the movement who later became known as "The Ogoni Nine" among them Ken Saro Wiwa, were arrested and accused of incitement to murder following the deaths of four Ogoni elders. Saro Wiwa and his comrades denied the charges but were imprisoned for over a year before being found guilty of the offence and were sentenced to death by a specially –convened tribunal, selected by General Sani Abacha on November 10, 1995. Indeed, the main struggle after Ogoni's turn towards organized activism in 1993 has been the demand for compensation from Anglo-Dutch oil giant Shell for pollution and environmental damage caused by the company's oil drilling and dilapidated pipeline infrastructure leading to devastating oil spills. Their protest was regularly met with strong counter-insurgency measures by the federal government and security agencies.

As of 2006, the situation in Ogoni land had eased significantly, assisted by the transition to democratic rule in 1999 (The Sunday magazine Lagos, May 15, 1994, pg.12 and Human Right Watch interview, Port-Harcourt, February 22, 1995).

Communication and National Security

The policy makers and executive branches may appear as the only key players in national decision based on their rise to power through force or election; however, the media plays a powerful role in national cohesion and

security. Aside from policies and military might often deployed by the government in addressing national security; communication is also vital in this mix, as information is a tool that can be used to protect the nation and achieve security or ruin it. The media is the mediator between a nation's government and its people. Hence, a nation's policies are transmitted and interpreted by the media. It is no surprise that in a democracy there is an emphasis on the freedom of the press to ensure that the media is free from selfish interests.

As indicated in Section 22 of the amended 1999 constitution of the Federal Republic of Nigeria, the media is entrusted with the power of monitoring governance and upholding fundamental objectives of state policy Ileonikhena, U. A. (2015, December 25).

It has been stated that the Vietnam War was compromised as a result of unfavorable media coverage leading to low levels of public support. In a democratic society, public support is key in the formulation and implementation of national policies (Momoh, J., 2016, January 13). As a watchdog, the media plays an important role in investigating, alerting and reporting individuals, activities and practices that can endanger the safety of the nation.

The advent of digital technology has also awakened citizen journalism and increased participation of the public in national affairs. Momoh (Momoh, J., 2016, January 13) quoting Shirky (2011) explains that social media has resulted in communal awareness of national issues and activities by using social networks to spread messages that can secure or destroy a nation as seen in the example of the Syrian nation who restricted its citizens from using Facebook. In 2012, Nigeria experienced the power of the media and citizen journalism when the "Occupy Nigeria" protests began on January 2nd as a response to the fuel subsidy removal by the federal government. Twitter was the main medium used in spreading information nationwide, resulting in many Nigerians participating in the protests and boycott from offices. Nigerians in other countries also showed solidarity by protesting in various locations worldwide (Heinrich Boll Stiftung, 2012, January). Ishaya Bako created an educative documentary called "Fueling Poverty" centered on the Occupy Nigeria protests; however, it was banned by the Nigerian Film and Video Censors Board (NFCVB) who described the content as "highly provocative and likely to encourage public disorder and undermine national security" (Atoke, 2012, May).

The #BringBackOurGirls Campaign is an example of a National Security issue that was spread all over the world through the help of social media with Hillary Clinton, Michelle Obama joining the campaign (Gibson, M., 2014, May 07). Traditional media also maintained the tempo through daily countdowns and editorials reminding the government on rescue efforts. As much as the new media has roused citizen journalism, it comes with its dangers including international terrorism and global crime syndicates. In this era of instant access to global information, new communication platforms and media technologies, there is a need to protect the nation by setting the right objectives; developing effective message and choosing appropriate channels to reach out to its citizens and its foreign counterparts.

Foreign media also plays a role in the national security of a nation, what is emphasized and highlighted can influence the perception of the country as a safe and peaceful nation or otherwise. The only way such reports can be countered is if national policies are continuously geared towards portraying the nation in a good light and rather than focusing on all its negatives, local media gives balanced reporting on both good and bad news.

National Security and Communication in the digital age

Technology is changing human patterns and habits globally; enabling the free flow of information within and outside nations as the weight, cost and power required for information-sharing technologies reduce. The complex nature of social networking creates room for multiple possibilities, both negative

and positive (Carafano, J., 2009). Its features create a virtual space for users to share information to the public and connect with others (Cooper, K., 2012). In the case of the Ebola and Zika Virus, the social media proved to be an effective tool in health-related crisis that was damaging to the security of a nation (Carafano, J., 2009). In the case of Reality Winner, a contractor with the National Security Agency (NSA) who allegedly leaked classified information on Russia's alleged attempts to influence the 2016 United States presidential elections to an online media outlet (Perez, E. et al., 2017). Social media is also subject to creating hoaxes that trend and can threaten the security of a nation, as social media platforms afford people the cloak of anonymity and breeds deception. Individuals can spread rumors without being traced, such stories can form the foundation of a national discourse even though it's based on falsehood (Catone, J., 2009).

National security is affected by social networking in terms of gathering and verifying intelligence/and information; assessing and influencing public opinion. As a medium backed by immediacy, sometimes stories spread without being confirmed. On December 2016, the president of the United States, Donald Trump tweeted "Today there were terror attacks in Turkey, Switzerland and Germany – and it is only getting worse. The civilized world must change thinking!", at this time, the motive for the attacks were yet to be confirmed as terrorist attacks and with a followership of over 35.8 million followers, his assumptions could fuel global security issues (Heer, J., 2016). It also involves sharing risk communications that can help citizens in emergency or pandemic situations; conducting research; developing policies; planning and execution of programs and conducting information operations (Carafano, J. 2009) all of which can be threatened or strengthened by a series of posts on digital platforms.

Communication and National Security: Tools of implication

The relationship between national security and communication is emphasized through the use of certain tools within the national eco-system, which influence the national dialogue and the security of the nation. Pictures: As the popular saying goes "a picture is worth a thousand words", the media has used striking images to reinforce or weaken national security. During and after the Second World War, the media employed visuals in constructing public opinion and emphasizing stereotypes and labels. Images on the war front were reprinted in the print and electronic media to create a certain impression of the "enemy"; thereby garnering support for government decisions and polices (Byars, N. B., 1994, April).

Headlines: The media has perfected the skill of using words to set the emotional atmosphere in nations. When combined with the frequency and positioning of these headlines or articles, the atmosphere is amended to fit the melody of the current issues within the nation even when the government tries to play hide and seek. A good example is the health situation of the Nigerian president, Muhammadu Buhari. As much as the government has tried to keep it under wraps, the media has tried to keep it on the forefront with headlines such as "Buhari's Health Most Searched on Google" (Odunsi, W., 2017, May 18), "Doctors refuse to give Buhari a clean bill of health", "Fresh Anxiety in Aso Rock over Buhari's health" (A. Adetayo, O., 2017, April 22).

Also, the words from the direct interviews conducted with concerned parties on national issues, help to further elevate or diminish National security. For example, the interview from older people that experienced the Biafran war reveal that most of them will prefer peace rather than the cessation of the Igbos from Nigeria based on their experiences. This information compared to supporters of Nnamdi Kalu helps to provide a balanced view for the public and for decision-makers to be more vigilant in taking decisions and seeking solutions.

Content: The media will always take a side or sell a concept with the stories published and broadcast. The media can reinforce religious, tribal and sectional loyalties, hence leading to

cultural insecurity, invasion and exultation of western values over local values. In September 2015, the Nigeria media reported that President Buhari had ordered the closure and relocation of the church at the presidential villa. However, the rumors were debunked by the special adviser of the president, Femi Adesina – further escalation of this matter by the media could have caused religious crisis in the nation [33]. National Security is also enhanced or threatened by other parties in the media such as the film and music industries based on the approach in which they address national issues such as smuggling, drug trafficking, cyber-crimes and natural disasters in their content.

Nwanne (Nwanne, B. U., 2014) analysed the reportage of the Nigerian media during the Ebola crisis in his study The media reportage of the Ebola crisis: lessons from Nigeria, through a random sampling of newspapers and magazines devoted to Ebola-related information. His results showed that efforts by the media helped in reducing the widespread of the disease, as state, national and private media adopted effective communication strategies such as translation of information in various languages, consistency to create awareness (Nwanne, B. U., 2014).

Conditions: This includes the time or space given to the news dependent on the medium used. For newspaper, the space and position of a piece of news can influence the public perception of the seriousness or triviality of the news. For television and radio, it can be the amount of time allocated to the information or the time in which the news is broadcasted. Some of the national dailies in Nigeria continued countdown to the rescue of the Chibok girls on their front page to remind readers and citizens of the need to bring the girls back home.

Effective Communication for National Security
Effective and strategic communication minimizes the threats to national security, promoting peace as effective communication is aimed at ensuring peace and security amongst all the stakeholders in a nation including citizens, media, other institutions and the government. Whatever is spread in the media usually influences the communication among various institutions in the nation including the family, educational institutions, religious groups and organizations. Therefore, it is important that the government of a nation pays attention to the way they handle information and quell crisis with their communication strategies (Comish, P. et al., 2011).
They include;

- Identify the target market: Diverse issues on national security affect various stakeholders in different ways. It is important to identify the audience receiving the message and understand their idiosyncrasies. For example, the messaging for the people in the oil areas in the Niger Delta will differ from the messaging targeted at Niger Delta indigenes in the diaspora.
- Consistency in messaging: Information can only be effectively transmitted when the messaging is consistent and directed at the target audience.
- Competence and credibility: The government must have efficient spokespeople that can effectively transmit information to various bodies and the populace to bridge the communication gap within a nation. These people or media whether on social media or in the press must be credible personalities that can be trusted in the local and global sphere as the information is only as good as the messenger. - Constant engagement of stakeholders: Communication is incomplete without feedback; every nation must take into cognizance all its stakeholders and streamline its messaging to fit each category. Monologues are rarely effective; rather there should be an exchange of information that results into reaction and suggestions that aid peace and security within and outside nations.

Involvement and participation of citizens: Feedback and interaction is also as important as passing information. Digital media has

proved effective in sourcing from feedback from citizens of all age groups, gender, status, educational levels and religious beliefs. It acts as a means of measurement and evaluation, testing the effectiveness of the information transmitted within groups or the media.

CAUSES OF SECURITY CHALLENGES

Inadequate technological apparatus: The weak security system in Nigeria could be attributed to inadequate digital facilities for the security arm of the government.

The porosity of the border has also contributed to the challenges of fighting banditry and terrorism in Nigeria. **An influx of small arms and weapons:** There has been an incremental influx of small arms and light weapons by (SALWs) into Nigeria from the Sahel since the fall of Gadhafi's regime in Libya (Gaye, 2018). Due to this arms and weapons end up in the hands of non-state actors like terrorists, bandits, armed robbers and militants who use them to terrorize individuals and rural dwellers. According to Adeniyi, in September 2018, military troops in joint operations with personnel of the Department of State Service (DSS) arrested two suspected illicit arms dealers along the Funtua Gusau road with 1,479 rounds of 7.62mm (special) ammunition, on their way to deliver the 10 weapons to armed bandits.

Poor attitude of security personnel: In many cases, security personnel assigned to deal with given security situations lack the trust and expertise to handle the situations. Instead of defending the national interest, and values, and protecting people from being harmed by criminals, they rather become saboteurs of government efforts, by supporting and fueling insecurity by either leaking vital security information. Even when these exist, some personnel get influenced by ethnic, religious or communal sentiment and are easily prejudiced by their interest in serving their people, rather than the nation (Achumba, Ighomereho, & Akpor-Rabaro, 2013).

Unemployment: The increasing rate of youth unemployment has contributed to the increase of security challenges and other vices in the country. Adagba, Ugwu & Eme, 2012; and Epron, 2019, noted that Nigeria's high rate of unemployment, particularly among the youth is what majorly prompts the jobless youths in the country to resort to violent crime like banditry and terrorism.

Poverty and Poor Governance: Poverty, poor governance and government insensitivity to the plight of the populace also contribute greatly to the escalation of terrorism, banditry and other forms of violent and non-violent activities in Nigeria. According to Adeolu, 2018, the failure of successive administrations in Nigeria to address the challenges of poverty bedeviling the nation has made life burdensome and only the fittest survive.

Attractive benefits: It was also discovered that because of the attractive benefits accruing from their nefarious activities, worst boys join these gangs in order to enrich themselves. They also construct illegal vehicle checkpoints on major supply and commercial routes in some of the countries, wear camouflage security agents' uniforms and attack vehicles travelling on major roads targeting commuters, security personnel and aid workers unleashing mayhem on the populace.

Cyberattack: This refers to the deliberate exploitation of computer networks as a means to launch an attack and such attacks are mainly to disrupt the proper functioning of targets which include computer systems and servers through the use of hacking, advanced threats to computers and so on.

CONCLUSION

In conclusion, the central point of this paper is that the proliferation of violence crises in Nigeria is precipitated by not having the element of listening, lack of political will, corruption, marginalization and insensitivity on the part of the government to evolve effective and appropriate strategies for conflict management including none adoption of well-crafted technological digital facilities in tackling the security challenges in the country. However, insurgency, secession, insecurity and agitation are as old as man and have been used

with impunity by many groups to achieve evil tendencies. It is pertinent to note that all the above squabbles have ridiculed the economic cum political strata of the nations. Thus, it is a global war that needs the collaborative efforts of everyone and all the countries of the world because security is everyone's business. Also, the ability of the Nigerian government and leaders to deploy adequate technological and media communication tools, apply effective communication, re-integrate the security personnel and the public to imbibe new ideas and creativity on the application of new security digital surveillance tools, manage both human, natural resources, formulate and implement better policies to create employment and other opportunities, and reduce over-reliance on the security personnel's manual actions will salvage the situation on the ground. Therefore, governments, groups, NGOs, individuals and media users should avail themselves of this facility to share information and curb insecurity in the country. This facility would further democratize terrorism and banditry information and accommodate the majority of non-English users into local, national, and global efforts to fight insecurity.

RECOMMENDATIONS

In other to win this battle, the following are recommended;

1. Procurement of well-crafted and advanced technological systems such as Robots (none- human-actors) machines, natural language processors (language translation and dialect software), Unmanned Aerial Vehicles (UAV) like drones, Digital Security Surveillance Systems (DSSS) such as closed-circuit television (CCTV), satellite dish etc. that also predate effective use of media communication through internet, online newspaper, social media, online Tv, Radio etc. These digital machines will help in the fight against terrorists, kidnappers and bandits in Nigeria with the assistance of trained security personnel by cutting- off or disabling their contacts and information platforms. These Artificial Intelligence machine tools are used in both unmanned spaces and public places among others. According to the United Nations Secretary-General, António Guterres cited in (Nsude, I., 2022), if harnessed appropriately, it can play a role in the fulfilment of the 2030 Agenda for Sustainable Development, bringing an end to poverty, protecting the planet and ensuring peace and prosperity for all.
2. The government should be proactive in the welfare of the citizens, and security agents and regular training of security personnel to meet the challenges.
3. Strategic communications and software that provide counter-narratives to terrorist propaganda may also be disseminated through the internet, in multiple languages, to reach a broad, geographically diverse audience.
4. Collaboration among national and international security agencies and adding security studies to the Educational Curriculum of the country,
5. Adhere to justice and equity in piloting the affairs of the country,
6. Equal appointment to political positions,
7. Empower and create equal job opportunities, empower the local communities to reach out to the aggrieved parties or perpetrators of the acts with a message of peace and reconciliation, dialogue and discussion as a communication technique and approach for settling squabbles in the country.

To foster national development and security, the followings are recommended;

- The media must understand the important role they play towards national security and its policies and actions should be geared towards its success.
- National leaders must understand that communication plays a vital role in national security, hence they must work together with the media on tactics that encourage development communication strategies that safeguard the nation.

- The media and other social institutions within the nation also have a role in educating citizens on the impact of their communications on social media platforms to the safety of the nation.

REFERENCES

Abdullahi, A. (2019). *Rural banditry, regional security, and integration in West Africa*. Journal of Social and Political Sciences, 2(3), 644-654.

Achumba, I. C., Ighomereho, O. S. & Akpor-Rabaro, M. O. M. (2013). *Security challenges in Nigeria and the implications for business activities and sustainable development.* Journal of Economics and Sustainable Development, 4(2), 2222-2855.

Adeniyi, O. (2018). *Beyond the banditry in Zamfara.* Retrieved from: https://www.thisdaylive.com/index.php/2018/04/05/beyond-the-banditry-in-zamfara/

Adagba, O., Ugwu, S. C. and Eme, O. I. (2012). *Activities of Boko Haram and Insecurity Question in Nigeria, Arabian Journal of Business and Management* Review, Vol. 1, No.9, 77-99. Africa News, 'Nigeria: Death of Boko Haram leader Shekau indubitably confirmed', 17 June 2021

Agbata, F. (2018). *Technology and national security*. Available at https://punchng.com/technology-and-nationalsecurity/. Accessed: 27 September, 2022.

Akin Ibidapo-Obe (2008). *The Utility of Close-Circuit Television (CCTV) in Intelligence Gathering by Security Operatives in Nigeria*. Proceedings of the conference on intelligent security, Lagos.

Asemah, E.S. (2011). *Selected Mass Media Themes*. Jos: Jos University Press.

Ate, A.A and Ikerodah, J.O (2012) *"Community Journalism in Nigeria: Global Technological Reflections"*. Journal of New Media Technology. New York: IITSE Vol 2. PP. 52-59.

Ball–Rocheach, S. & DeFleur, M. (1976). *A dependency model of mass media. Communication Research*.

Brown, I., Korff, D. 2009. "*Terrorism and the Proportionality of Internet Surveillance*." European Journal of Criminology 6 (2): 119–34.

Brown, H (2010, September 24). *Thinking about national security: defence and foreign policy in a dangerous world*. In C.A Watson (Ed.), National security: a reference handbook. Retrieved from http:// www.wkipedia.org/national security.

Castells, M. 2011. The Rise of the Network Society: The Information Age: Economy, Society, and Culture, vol. 1. West Sussex, UK: John Wiley & Sons.

Campbell, J. (2018). *Terrorists are not the only ones exploiting ungoverned spaces across Nigeria.* Available at: https://www.cfr.org/blog/terrorists-are-not-only-onesexploiting-ungoverned-spaces-across-nigeria. Accessed: 31 October 2022.

Campbell, H. & Rotberg, R. I. (2021). *Nigeria is a failed State*, Retrieved on 9 of September, 2021 from https://foreignpolicy.com/2021/05/27/nigeria-is-a-failed-state/

Chamberlain, C. (2018). *How are drones changing warfare, and threatening security*. Available at: from https://news.illinois.edu/view/6367/645164. Accessed: October 20, 2022.

CNN News. *Boko Haram Fast Facts*. Available from: https://www.edition.cnn.com/2016/06/09/world/boko-haramfast-facts/index.html.

Council on Foreign Relations (2020). *Banditry violence and displacement in the Northwest.* ACAPS Briefing Note: Conflict, July 24, 2020, 1-3. Retrieved from: https://www.acaps.org/country/Nigeria/crisis/northwestbanditry

Duyile, D. (2015) *Writing for the Media – A manual for African Journalists*. Lagos: Gong Communication Ikiebe and Development Studies, 7(2), 141-

Country Policy and Information Note Nigeria: Islamist extremist groups in North East Nigeria Version 3.0 July 2021.

Dennis, E.E. & Defleur, M.L. (2010) *Understanding media in the Digital Age* New York: Pearson.

Encyclopaedia Britannica (2005). *Britannica Concise Encyclopedia*. Encyclopaedia Britannica, Incorporated.

Epron, S. (2019). *Emerging security threats: Factors and implications for Nigeria"s socio-economic development 2015-2019*. Journal of Economics.

Akpama, E. (2013). Counselling for effective communication: A tool for national security. Journal of Education and Practice, 4(7), 31-36.

Comish, P., Lindley-French, J., & Yorke, C. (2011). Strategic communications and national strategy. The Royal Institute of International Affairs. London: Chatham House Report.

Archetti, C. (2015). Terrorism, communication and new media: Explaining radicalization in the digital age. Perspectives on terrorism, 9(1).

Igwebuike, E. (2016). A pragma-semiotic analysis of "occupy Nigeria group" online posts on the 2012 fuel subsidy removal in Nigeria. Journal of Visual Literacy, 35(3), 201-214.

International Centre for Counter-terrorism - The Hague. (2014). About fear, terrorism and what is really new. Retrieved from International Centre for Counter-terrorism: https://icct.nl/publication/about-fear-terrorism-and-what-is-really-new/

Makinda, S. (1998). Sovereignty and global security, security dialogue. Sage Publications, 29(3), 281-292.

Momoh, J. (2016, January 13). Information as a Tool for National Security: Role of the Media

CRYPTOLOGY AND SECURED COMMUNICATION

Adebayo Akinade dfisn & Adesola Fagbemi

ABSTRACT

In the realm of digital communication, cryptography stands as the guardian of privacy, integrity, and authenticity. From ancient substitution ciphers to modern asymmetric encryption algorithms, the evolution of cryptology has been instrumental in safeguarding sensitive information. This paper explores the historical roots and modern applications of cryptography, shedding light on its pivotal role in securing electronic communications and transactions.

Beyond the algorithms and protocols lies the critical framework of security documentation. Comprehensive documentation is the cornerstone of effective information security management, covering policies, responsibilities, systems, audits, and compliance. It serves as a roadmap for security officers, guiding them in navigating the complex landscape of cybersecurity threats and regulations.

Furthermore, this paper highlights the symbiotic relationship between cryptography and security documentation. While cryptography provides the tools for encryption and authentication, security documentation ensures accountability and transparency in implementing and maintaining security measures. Together, they form the bedrock of information assurance in an interconnected world, where digital threats abound and privacy concerns loom large.

In conclusion, the paper underscores the imperative of embracing both cryptography and security documentation in the quest for robust digital protection. By understanding their intertwined significance and embracing best practices in both domains, organizations can fortify their defenses against cyber threats and uphold the trust of their stakeholders in an increasingly digitized society.

KEYWORDS:

Cryptology, Security Documentation, Information Assurance, Risk Assessment

INTRODUCTION

“Kryptos” is a Greek word meaning "hidden". These days of the Internet and Information explosion, scientists are looking more and more at the use of cryptographic aids as a means of safeguarding and regulating access to information" or providing security from hackers.

In the history of cryptography, it was necessary for the recipient to have the same key as the sender in order to be able to understand the message. There is the story of Julius Caesar (100 to 44BC), for example, who encrypted his secret messages by displacing each letter by three places in the alphabet, so that an "A" became a "D" E becomes "H" and so on. Yet much more complicated codes can be cracked.

In World War II, for example, the English managed to crack the code used by the German Military which was generated by the cryptographic machine known as Enigma the word is from these Greek word " hidden" used an algorithm, or a schematized mathematical process, to transpose each letter in another according to a secret code.

Data Encryption Standard (DES) is an international system that has proved its worth over several decade The DES uses 256 algorithms, which translate into more than 72 quadrillion opportunities for encryption a figure, which experts say is now too small. And while digitization that breaks down characters Wm binary codes, has made encryption procedures faster, they have nevertheless become more secure.

The immense public use of electronic communications and the radical vulnerability of the latter have now given cause for thought. There are two main criteria to be met, for easy

operation of the system. Ids recipient must be sure that the sender is really the person that he or she claims to be and the data must arrive in an uncorrupted form.

Further developments that have led to the discovery of so-called technology look promising. The key aspect of the procedure is the IIIMI of two separate keys, one for encoding and the other for decoding. The public key, which may really be open and perfectly public, is used to encrypt a normal piece of text. The recipient of the message, however needs a private key that can be used to generate an electronic signature, while the public key can only be used to check its authenticity. Usually, the keys are joined together and assigned to a single person by a so-called trust center. The encoding-decoding procedure can run with the help of appropriate software on a standard personal computer.

As a response to increase in demand for keys and greater digital storage required, the RSA (i.e. Ronald Rivest Shamir and Leonard Adleman) procedure, which is based on the multiplication of primary numbers containing from two to 170 digits has been devised. This makes it extremely difficult for hackers to resolve the product back into its factors. As a result of increase in data, the data storage space occupied by such monstrous numbers continues to grow. Also, the electronic eavesdroppers have access to more sophisticated technology and this has led to the increasing development of cryptographic procedures based on elliptic curves.

The advantage of the use of such elliptic curves is that it requires shorter key with enhanced security and reduced data storage. With the help of an elliptic curve, an RSA key with a length of 2048 bits would shrink to a mere 200 bits (10% of its size). The new technique is so powerful that it would be possible to encrypt information in such a complex manner that not even all the computers in the world working in parallel would be able to decipher the message.

That is comforting for companies, individuals and governments particularly since it is believed by many experts that within the next five years, electronic signature will be available across a broad range of areas. This will in turn serve to facilitate a whole range of applications, many of which will make use of personal data.

As the world of the Internet continues to expand, the natural one gets smaller as well as faster. In the days of old, the opposite was the truth. When the need arose to convey sensitive information, the general would first order a messenger to shave his head. Afterwards the missive would be tattooed into his bald plate. In order to be able to discover the secret information; what the recipient needed to do was to order the messenger to shave again. However, before the original message could even be sent, it was necessary to wait a few weeks for the emissary's hair to grow back, enough to hide it.

CRYPTOLOGY

This is the science and art of writing and sending messages in code form. The following is a simple aspect of a more sophisticated cryptography taken from Why We Struck by Major Adewale Ademoyega, formerly of the Nigerian Army. (cf. [1]). As reported in that book, on January 13, 1966 Major Ademoyega sent the following coded message from Lagos to Major Kaduna Nzeogwu in Kaduna:

"Major Ademoyega will leave Lagos after forty-one days holiday and will arrive in Kaduna after fifty-one days".

COUNTER-MEASURES IN DEFENCE

Cost-Effectiveness

In deciding what information needs to be protected, remember that security must be cost-effective. In the protection of secrets, the cost of the damage must be assessed in the light of the money, time and effort spent on protection.

Secrets are an asset and their protection can form an integral part of the overall security (and often fire control) plan. Remember that information is definite, valuable and

irrecoverable, unlike physical items which can be recovered.

Try to relate protection measures taken to the protection of employees, plant and machinery. In some cases, for example, fire prevention measures will be improved and part of the cost will be offset by reduced insurance premium rates. An example of the benefits which can accrue from the installation of an effective access control system providing proper identification of employees and visitors is given as a costing example.

Let us say that the total initial cost of N30 000. This will include card readers; photograph bearing identity cards (laminated), a visitor's pass system and restriction of access to certain parts of the premises.

Examine the systems on offer before you decide which one to opt for, and then add to them the additional facilities which will save money. Most of the sophisticated systems on offer can accommodate payroll computation, overtime worked and limitation thereof, and provide up-to-the-minute strengths, absentees, personnel details and other printouts.

Design the Systems

Bear in mind that any system must be simple, easy to operate and must be acceptable to those it is designed to control and protect. It must also be sufficiently flexible to suit rapidly changing circumstances.

Put in systems slowly and remember that once a system is installed, it must work efficiently or credibility is lost. Once a system has to be dropped, authority in undermined.

Review Systems Regularly

Technological advances can render existing systems obsolete or provide new and additional facilities which are invaluable in cost saving and increased efficiency. Any security practitioner worth his salt will ensure that he receives book lists, magazines and film catalogues to enable him to keep abreast of developments in the protection field.

Sensors, infra-red systems, acoustic alarms, radio communications, perimeter alerts, fibre-optics and a host of similar items are the tools available to the security man to do his job, and these are constantly being improved, reduced in size, and often in cost.

Counters to Electronic Surveillance

A wide range of electronic equipment are readily available in Nigeria for both attack and defence, yet there are few people sufficiently qualified to be able to counter this threat effectively. The amateur can so easily hoodwink the customer into thinking that the threat has been removed and the area "declared safe" when, in fact, the more sophisticated devices, present have been overlooked. The result of this is that precautions taken when suspicion of "bugging" are dropped and the spy reaps his rich harvest. The professional in the field of electronic anti-espionage measures are the people who continually keep abreast of developments in this field and whose track record speaks for themselves. A problem which has recently arisen in this field is the proliferation of readily available sources of information on "How to steal your neighbor's secrets. Numerous publications are available "over the counter" and this author, at moderate cost, in answer to a magazine advertisement, obtained a 153-page document from an American company of repute outlining in detail the full range of surveillance methods available. Diagrams, charts and detailed installation instructions for each type of equipment were also included. Microwave transmitters, parabolic refectory, laser beams, non-coherent light beams, carrier current transmitters, aspirin table miniature "drop in" transmitters and passive cavity transmitters were but a few of the items available, with full instructions as to use and installation.

CRYPTOGRAPHY IN THE MODERN AGE

After World War 2, the electronics that had been developed in support of radar were adapted to cryptomachines. The first electrical cryptomachines were little more than rotor machines where the rotors had been replaced by electronic substitutions. The only advantage of these electronic rotor machines

was their speed of operation and they inherited the inherent weaknesses of the mechanical rotor machines.

There is little information available regarding the secret cipher machines of the 1960s and it is likely that this subject will remain the shrouded in rumour until the relevant information is de-classified.

The era of computers and electronics has meant an unprecedented freedom for cipher designers to use elaborate designs which would be far too prone to error if handled by pencil and paper, or far too expensive to implement in the form of an electromechanical cipher machine. The main thrust of development has been in the development of block ciphers, beginning with the LUCIFER project at IBM, a direct ancestor of DES (Data Encryption Standard).

CRYPTOGRAPHY

Cryptographic systems are generally grouped according to three facts about them:

1. The mathematical operation that changes the plaintext into the ciphertext.
2. Whether a block or a stream cipher is produced.
3. The type of key system used - single or two key.

Single Key Cryptography

SUBSTITUTION CIPHERS

A substitution cipher is one in which the units of the plaintext (usually letters or numbers) are replaced with other symbols or groups of symbols. The actual order of the units of the plaintext is not changed.

The simplest substitution cipher is one where the alphabet of the cipher is merely a shift of the plaintext alphabet, for example, A might be encrypted as B, C as D and so forth. Of this type of cipher, the most well-known is the Caesar cipher, used by Julius Caesar in which A becomes **D** etc. It is easy to guess that cyclical-shift substitution ciphers of this sort are not at all secure because individual letter frequencies are left completely intact.

There are primarily two approaches that have been used with substitution ciphers to reduce the extent to which the structure of the plaintext, including the letter frequencies, survives into the ciphertext. One of these methods is to treat more than a single letter as one element i.e. two or three successive letters are treated as one unit. The other method is to use several different cipher alphabets.

Charles Wheatstone was a 19th century English physicist, born on February 6th, 1802. Apart from devising the Playfair cipher, he also invented the Wheatstone bridge, a device for accurately measuring electrical resistance which became widely used in laboratories. He also initiated the usage of electromagnets in electric generators and devised the stereoscope, a device for viewing pictures in three dimensions still used today. The Playfair cipher was named for Lyon Playfair, the first Baron Playfair of St. Andrews, who championed its usage at the British Foreign Office (although he was unsuccessful).

Here is an example of a Playfair cipher. The aid used to carry out the encryption is a 5 x 5 square matrix similar to a Polybius checkerboard in that it contains all the letters of the alphabet (1 and J are treated as the same letter); however, a keyword is placed first and then the remaining letters are placed in alphabetical order.

If the plaintext contains an odd number of letters, then an X is appended to the last word to make it an even number. Also, if any of the digraphs consist of identical letters e.g. SUMMER, then an extra letter is placed between them.

The first step in performing the encryption is to locate the two letters from the plaintext in the matrix. There are then several different substitution rules depending on their positioning:

If the pair of letters are in different rows and columns. The rows of the ciphertext letters are kept the same as the rows of the plaintext letters, however the columns swap. Therefore ME, once encrypted, becomes SC because E

changes to the letter which is in the same row (2) but in the column of M (1) and M changes to the letter which is in the same row (1) but the column of E (3). It may be easier to remember this as the plaintext letters being at two corners of a rectangle and the ciphertext letters being at the other two corners.

If the pair of letters are in the same row. The ciphertext letters are the letters to the right of the plaintext letters. For example, T and A are in the same row so T will encrypt to S and A will encrypt to B, forming SB.

If the pair of letters are in the same column. The ciphertext letters are the letters below the plaintext letters. For example, Y and L are in the same column so Y becomes A and L becomes R., forming AR.

Thus, we can now encrypt the phrase “Merchant Taylors’ School”:
Plaintext: ME RC HA NT TA YL OR SZ SC HO OL
Ciphertext: SC OF LM BI. AB AR PU BX ME OV RH
(The last S of "TAYLORS" is paired with a Z to separate it from the first S of "SCHOOL").

The other approach to concealing plaintext structure in the ciphertext involves using several different substitution ciphers. The resulting ciphers, which are generically known as polyalphabetic, have a long history of usage. The best-known polyalphabetic ciphers are the simple Vigenère ciphers which are named after the 16th century French cryptographer Blaise de Vigenère (see History). Blaise de Vigenère actually produced a more sophisticated autokey cipher, but through an accident of history, his name has become attached to this weaker cipher.

For many years this cipher was thought to be impregnable and it was rumoured that a well-known scientific magazine pronounced it "uncrackable" as late as 1917, despite the fact that it had been broken by then.

In the simplest system of the Vigenère type the key is a word or a phrase which is repeated over and over again. The plaintext is encrypted using the table shown as Figure 4. The ciphertext letter is found at the intersection of the column headed by the plaintext letter and the row indexed by the key letter. To decrypt the plaintext letter is found at the head of the column determined by the intersection of the diagonal containing the cipher letter and the row containing the key letter.

It is the periodicity of the repeating key which leads to the weaknesses in this method and its vulnerabilities to cryptanalysis. This periodicity of a repeating key can be eliminated by the use of a running-key Vigenère cipher, produced when a non-repeating key is used. However, even though running-key ciphers eliminate periodicity, it is still possible to cryptanalyze them by means of several methods. However, the job of the cryptanalyst is made much harder and a cryptanalyst would require a much larger segment of ciphertext to solve a running-key cipher than one with a repeating key. In fact, the work of Major Joseph Mauborgne of the U.S. Army eventually led to the realisation that the only cryptographic system that is totally secure is that with a one-time completely random key.

Here is how the words "Merchant Taylors School" can be encrypted using this cipher:

Plaintext: MERCHANT TAYLORS SCHOOL
Key: DONTSTAN DALONED ONTST
Ciphertext: PSEVZTNG WAJZBVV GPAGH

Transposition Ciphers

Transposition ciphers rearrange the letters of the plaintext without changing the letters themselves. For example, a very simple transposition cipher is the rail fence, in which the plaintext is staggered between two rows and then read off to give the ciphertext. In a two-row rail fence the message MERCHANT TAYLORS' SCHOOL becomes:

M R H N T Y O S C O L
E C A T A L A L R S H O
Which is read out as: MRHNTYOSCOLECATALRSHO.

The rail fence is the simplest example of a class of transposition ciphers called route ciphers.

These were quite popular in the early history of cryptography. Generally, in route ciphers the elements of the plaintext (usually in this case single letters) are written on a pre-arranged route into a matrix agreed upon by the transmitter and receiver. The example above has a two row by n-column matrix in which the plaintext is entered sequentially by columns, the encryption route is therefore to read the top row and then the lower.

Obviously, to even approach an acceptable level of security, the route would have to be much more complicated than the one in this example. One form of transposition that has enjoyed widespread use relies on identifying the route by means of an easily remembered keyword. This can be done in several ways. One way, as in this example, is to define the order in which each column is written depending on the alphabetical position of each letter of the keyword relative to the other letters.

Using the keyword CIPHER, a matrix can be written out like the one below:

C	**IP**	**H**	**E**	**R**
1	**45**	**5**	**3**	**6**
M	ER	R	C	A
N	TT	T	A	L
O	RS	S	S	H
O	OL	Z	Z	Z

Unlike the previous example the plaintext has been written into the columns from left to right as normal, and the ciphertext will be formed by reading down the columns. The order in which the columns are written to form the ciphertext is determined by the key.

This matrix therefore yields the ciphertext: MNOOHYCZCASZETRORTSLALHZ.
The first column is first because C is the earliest in the alphabet, followed by the second to last column because E is the next in the alphabet.

The security of this method of encryption can be significantly improved by re-encrypting the resulting cipher using another transposition. Because the product of the two transpositions is also a transposition, the effect of multiple transpositions is to define a complex route through the matrix which would not by itself by easy to define with a simply remembered mnemonic. When decrypting a route cipher, the receiver simply enters the ciphertext into the agreed-upon matrix according to the encryption route and then simply reads out the plaintext.

In modem cryptography transposition cipher systems serve mainly as one of several methods used as a step in forming a product cipher.

Product Ciphers

In the days of manual cryptography i.e. without the aid of a computer product ciphers were a useful device for the cryptographer and double transposition ciphers on keyword-based matrices were, in fact, widely used. There was also some use of a particular class of product ciphers called fractionation systems. In a fractionation system a substitution is first made from symbols in the plaintext to multiple symbols (usually pairs, in which case the cipher is called a biliteral cipher) in the ciphertext, which is then super encrypted by a transposition.

One of the most famous field ciphers ever was a fractionation system ¬the ADFGVX cipher which was employed by the German Army during the First World War. This system was so named because it used a 6 6 matrix to substitution-encrypt the 26 letters of the alphabet and 10 digits into pairs of the symbols A, D, F, G, V and X. The resulting biliteral cipher is only an intermediate cipher, it is then written into a rectangular matrix and transposed to produce the final cipher which is the one which would be transmitted.

Here is an example of enciphering the phrase "Merchant Taylors" with this cipher using the key word "Subject".

AD	F	G	V	X	
A	SU	B	J	E	C
D	TA	D	F	G	H
F	IK	L	M	N	O
G	PQ	R	V	W	X
V	YZ	0	1	2	3
X	45	6	7	8	9

Plaintext: M E R C H A N T
T A Y L O R S

Ciphertext: FGAV GF AX DX DD FV DA DA DD VA FF FX GF AA

This intermediate ciphertext can then be put in a transposition matrix based on a different key.

C	**IP**	**H**	**E**	**R**
1	**45**	**3**	**2**	**6**
F	GA	V	G	F
A	XD	X	D	D
F	VD	A	D	A
D	DV	A	F	F
F	XG	F	A	A

The final cipher is therefore: FAFDFGDDFAVXAAFGXVDXADDVGFDAFA.

Block Ciphers

Generally, ciphers transform pieces of plaintext of a fixed size into ciphertext. In older, manual systems, these pieces were usually single letters or characters (or sometimes, as in the Playfair cipher, digraphs), since these were the largest units that could be easily encrypted or decrypted by hand. Although systems which operated on sets of three characters and other, larger groups of numbers, were proposed and understood to potentially be more secure they were never implemented because of the extra difficulty in the manual encryption or decryption process. In modern, single key cryptography however, the units of information can be much larger.

A block cipher is a type of symmetric-key encryption algorithm that changes a fixed-length block of the plaintext into the same length of ciphertext. The encryption works by means of a key. Decryption is simply the reverse of the encryption process using the same secret key. The fixed length is called the block size and for modem block ciphers is usually 64 bits. As processors become more sophisticated, however, it is likely that this block size will increase to 128 bits.

Since different plaintext blocks are mapped to different ciphertext blocks, a block cipher effectively provides a permutation of the set of all possible messages. The actual permutation produced during any particular operation is of course secret, and determined by the key.

An iterated block cipher encrypts a plaintext block using a process with several stages (rounds). At each stage the same process (known as a round function) is applied to the data using a subkey (the set of subkeys usually being derived from a user provided key). The number of rounds in an iterated block cipher depends on the desired security level of the encrypted ciphertext and the trade-off that must be made with performance; fairly obviously an iterated block cipher with a large number of rounds will require more processing time. It is worth noting that in some cases the number of rounds required to provide an accurate level of security will be too large for the cipher to be practical.

An example of an iterated block cipher is a Feistel cipher. Feistel ciphers are a special class of iterated block ciphers. In this type of cipher, the ciphertext is calculated from the repeated application of the same round function.

Stream Ciphers

A stream cipher also breaks the plaintext into units, this time it is normally a single character. It then encrypts the nth unit of the plaintext with the nth unit of the key stream. Stream ciphers can be designed to be exceptionally fast, much faster than any block cipher. While the encryption of any particular plaintext with a block cipher will result in the same ciphertext when the same key is used; with a stream cipher, the transformation of the smaller plaintext units will vary, depending on when they are encountered during the encryption process.

A stream cipher generates what is known as a key stream - a sequence of bits, which is used as a key. The encryption process involves combining the key stream with the plaintext.
The key stream can be generated in two ways:

- Independent of the plaintext and cipher text (this yields what is known as a synchronous stream cipher).

- Depending on the data and its encryption (in which case the stream cipher is said to be self-synchronizing).

The majority of stream cipher designs are for synchronous stream ciphers.

Interest in stream ciphers is currently attributed to the appealing properties of the one-time pad. A one-time pad, which is sometimes called the Vernam cipher, uses a key stream which is the same length as the plaintext message and consists of a series of bits generated completely at random. Theoretically this should produce cipher text which, is the most secure possible, because since the key stream is random even a cryptanalyst with infinite computational resources can still only guess at the underlying plaintext. While the one-time pad has occasionally seen use in wartime for ultra-secret transmissions the fact that the key is as long as the message introduces severe practical problems and so, while theoretically perfectly secure, the one-time pad is generally impractical. Stream ciphers were developed as an approximation to the one-time pad.

At this time, there is no *de facto* standard for stream ciphers although the most widely used stream cipher is RC4, a stream cipher designed by Rivest for RSA Data Security Inc. It is a variable key-size stream cipher with an algorithm based on the use of a random permutation.

Strangely, certain modes of operation of a block cipher transform it into a key stream generator and so, in this way, any block cipher can be used as a stream cipher. Stream ciphers with a dedicated design and typically much faster, however.

One method for generating a key stream is a Linear Feedback Shift Register (LFSR). This is a mechanism for generating a sequence of binary bits. LFSRs are easy to implement and fast operating in both hardware and software however a single LFSR is not secure because over the years, a mathematical framework has been developed which allows for the analysis of their output.

This example used small primes so it can be seen that the product, n, is not at all difficult to factor to retrieve the original primes. In using RSA, it has always been suggested to use "strong" primes which have certain properties making their product especially difficult to factor using certain factoring methods. However, advances in factoring techniques over the last decade have near completely negated the advantage of strong primes, the elliptic curve factoring algorithm is one such advance. Therefore, it is not choosing traditionally "strong" primes which matters but rather choosing large primes.

In 1997, a specific assessment of the security of 512-bit RSA keys shows that one may be factored for less than $1,000,000 in cost and eight months of effort. It is therefore believed that 512-bit keys provide insufficient security for anything other than short-term needs. RSA Laboratories currently recommends key sizes of 768 bits for personal use, 1024 bits for corporate use, and 2048 bits for extremely valuable keys like the root-key pair used by a certifying authority. Security can be increased by changing a user's keys regularly and it is typical for a user's key to expire after two years (the opportunity to change keys also allows for a longer length key to be chosen).

It should be noted that the key sizes for RSA (and other public-key techniques) are much larger than those for block ciphers like DES, but the security of an RSA key cannot be compared to the security of a key in another system purely in terms of length. It should also be noted that although increasing the length of the modulus may increase the security of the system it also significantly increases the amount of time required to perform encryption, decryption and authentication - doubling the modulus will, on average, quadruple the amount of time taken for encryption and increase the time taken for decryption by a factor of eight.

"Real World" Usage of The RSA Algorithm
DES, and other block ciphers, are much faster in operations than RSA. Typically, in software, DES is approximately 100 times faster than RSA and in hardware can be between 1000 and

10000 times faster depending on the implementation. Because of the length of time taken for public key encryption a public key system such as RSA is often used in conjunction with a secret-key system such as DES. In this case the message is encrypted with a randomly chosen DES key and the key itself is encrypted and sent with RSA. This method combines the low number of keys required for RSA with the high-speed operation of DES.

RSA is the most widely used public-key cryptosystem available currently and has often been referred to as a de-facto standard regardless of official recognition. In fact, RSA is part of many official standards worldwide. These include ISO 9796 which lists RSA as a compatible cryptographic algorithm and many internet standards and proposals including S/MIME.

Cryptography in the "Real World"

Applications Of Cryptography

In the information dependent world in which we now live cryptography can be found all around us, often in places where you would not expect it. When people think about encryption, they tend to think about vast computer banks processing military and diplomatic communications, or a World War two rotor cipher machine slowly deciphering an order. In reality, cryptography - although obviously essential for the military and diplomatic services - has many commercial uses and applications.

From protecting confidential company information, to protecting a telephone call, to allowing someone to order a product on the Internet without the fear of their credit card number being intercepted and used against them, cryptography is all about increasing the level of privacy of individuals and groups. For example, cryptography is often used to prevent forgers from counterfeiting winning lottery tickets. Each lottery ticket can have two numbers printed onto it, one plaintext and one the corresponding cipher. Unless the counterfeiter has cryptanalyzed the lottery's cryptosystem, he or she will not be able to print an acceptable forgery.

In a world where virtually all data of any importance is held on ft computer system the necessity of cryptography cannot be disputed.

Politics Of Cryptography

Widespread use of cryptosystems is something most governments not particularly happy about - precisely because it threatens to give more privacy to the individual, including criminals. For many years, police forces have been able to tap phone lines and intercept mail, however, in an encrypted future that may become impossible.

This has led to some pretty strange decisions on the part of governments, particularly the United States government. In the United States, cryptography is classed as a munition and the export of programs containing cryptosystems is tightly controlled. In 1992, the Software Publishers Association reached agreement with the State Department to allow the export of software that contained RSA's RC2 and RC4 encryption algorithms, but only if the key size was limited to 40 bits as opposed to the 128-bit keys available for use within the US. This significantly reduced the level of privacy produced. In 1997 this was increased to 56 bits. The US government has proposed several methods whereby it would allow the export of stronger encryption, all based on a system where the US government could gain access to the keys, if necessary, for example the clipper chip.

The resolution of this issue is regarded to be one of the most important for the future of e-commerce.

Cryptanalysis

It is beyond the scope of this essay to deal with all types of cryptanalyses so I will give a brief overview and an example of where cryptanalysis has been successful. Unlike cryptography which is a clearly defined science, cryptanalysis is as much an art as it is a science. Success in cryptanalyzing a cipher is a flash of inspiration almost as often as it the result of using cryptanalysis techniques alone.

Types of Cryptanalyses

There are several distinct types of cryptanalytic attack. The type used depends on the type of cipher and how much information the cryptanalyst has.

Types Of Cryptanalytic Attacks

A standard cryptanalytic attack is to determine the key which maps a known plaintext to a known ciphertext. This plaintext can be known because it is standard or because it is guessed. If the plaintext segment is guessed it is unlikely that its exact position is known however a message is generally short enough for a cryptanalyst to try all possible positions in parallel. In some systems a known ciphertext-plaintext pair will compromise the entire system however a strong encryption algorithm will be unbreakable under this type of attack.

A brute force attack requires a large amount of computing power and a large amount of time to run. It consists of trying all possibilities in a logical manner until the correct one is found. For the majority of encryption algorithms, a brute force attack is impractical due to the large number of possibilities.

Another type of brute force attack is a dictionary attack. This essentially involves running through a dictionary of words in the hope that the key (or the plaintext) is one of them. This type of attack is often used to determine passwords since people usually use easy to remember words.

In a ciphertext only attack the cryptanalyst has only the encoded message from which to determine the plaintext, with no knowledge whatsoever of the actual message. A ciphertext only attack is presumed to be possible, if not easy. In fact, an encryption techniques resistance to a ciphertext only attack is considered the basis for its cryptographic security.

In a chosen plaintext attack the cryptanalyst has the capability to find the ciphertext corresponding to an arbitrary plaintext message of his or her own choosing. The likelihood of this type of attack being possible is not much. Codes which can survive this attack are considered to be very secure.

In a chosen ciphertext attack the cryptanalyst can choose an arbitrary ciphertext and find the corresponding decrypted plaintext. This attack can be used in public key systems, where it may reveal the private key.

In an adaptive chosen plaintext attack the cryptanalyst can determine the ciphertext of chosen plaintexts in an iterative process based on previous results. This is the general name for a method of attacking product ciphers called "differential cryptanalysis".

Frequency Tables

The cryptanalysis of single-key cryptosystems depends on one simple fact - that some traces of the original structure of the plaintext may be visible in the ciphertext. For example, in a monoalphabetic substitution cipher where each letter in the plaintext is replaced by a letter in the ciphertext which is the same each time, a simple analysis of a sizeable portion of ciphertext can be used to retrieve most of the plaintext.

Here is a monoalphabetic substitution cipher of a random paragraph of English:
UFMDHQAQTMGRG BX GRAZTW PWM
UFMDHBGMGHWOG VWDWAVG BA BAW
GRODTW XQUHAQOWTM HCQH FIFQU W G
BX GHFIUHIFW BF DQHTIWFA RA HCW
DTQRAHWLH OQM GIFJRJW WAUFMDHRBA
QAV SW VRGUWFARSTW RA HCW
URDCWFHWLH.

W occurs 20 times in the cipher, H occurs 16 times. From this information and using the frequency table to the left it would be possible for a cryptanalyst to recover the majority of the plaintext.

The usefulness of analyzing the structure of the ciphertext can be reduced by any encryption procedure that attempts to disguise the structure. However, eliminating the underlying structure is harder than it would first seem. Digraphs, for example, show a strong frequency distribution - TH occurs very often, about 20 times more often than HT

and so on. With tables of digraph frequencies, it is possible to recover the underlying plaintext, however, the amount of ciphertext required would be much greater.

In the heyday of manual cryptanalysis, huge volumes of word patterns were compiled. Although these only contained the most obvious and easily recognised word patterns they were still of importance if they could provide that vital clue which could break the entire cipher.

Cryptanalysis Of Public Key Ciphers

Public key cryptography requires a fundamentally different type of cryptanalysis than is used for single key cryptanalysis. Because public key cryptography relies on "hard" mathematical problems, their cryptanalysis is essentially research into solving the underlying mathematical problems. Cryptanalysis of public key ciphers is therefore virtually indistinguishable from research into any other area of mathematics.

For example, to "crack" the RSA algorithm and obtain the private key from the public key would essentially involve research into factoring algorithms. Factoring is a very active field of research among mathematicians and computer scientists. The best general-purpose factoring is algorithm today.

SECURITY DOCUMENTATION: PRACTICES AND TECHNIQUES

ADEBAYO AKINADE dfisn And David Okwun KALU fisn

Introduction

The word *'documentation'* originates from "document" which means written evidence confirming a legal state, a fact or a state, which is the materially recorded expression of human thought. In a general term, a document may be defined as recorded information.

This is a broad meaning; documents are not only printed matter and manuscripts, which contain verbal expression. Texts recorded by means of graphic signs are also documents. Graphic documents include maps, illustrations, drawings, photographs, films, records and tape recordings of voice or sound. All museum items: pictures, sculptures, models, medals, seals, collections of natural science specimens are also examples of documents.

Documentation is an activity connected with documents as a basis of historical works and in reports. It is a collection of documents for various purposes.

Organisational security officers are charged with ensuring the security of information assets and systems. As such, they are perilously located between management and technology. They are required to ensure that the technological systems are implemented and operated in such a manner, that the business risk to organisational information assets and systems is contained within acceptable boundaries. In effect they are required to assess the level of business risk from an information security viewpoint, and to recommend operational or technical changes designed to bring that risk down to some acceptable, but often unspecified, level.

Subjective risk assessments bode ill for a security officer in a highly complex, networked environment, particularly when information security failures may have significant impacts on the financial well-being or the regulatory or contractual obligations of that organisation. In the aftermath of a serious information security failure, security officers may well be called upon to supply convincing, documented, evidence that their risk assessment recommendations, to senior management, were well founded.

Information security management standards, such as German IT Baseline Protection Manual Standard Security Safeguards [3], BS7799 [4] and ISO17799 [5] do provide an infrastructure of information security management and hence some guidance on the structure of security documentation. Nevertheless, it is interesting to compare the emphasis on bookkeeping in the training of financial auditors, with the average educational/training courses for security personnel. In general, there is a significant lack of guidance, let alone tools to aid the security officer in the documentation task.

The security officer can take out insurance and persuade management to fund a compliance audit. The results of such an audit will enable the security officer to either:

- Display a certificate on the wall, or
- Present management with a list of resources necessary to acquire such a certificate.

A security incident could cause serious financial losses to an organisation, its partners and clients. In these litigious days, the security officer could well face a hostile barrister, in the aftermath of such a security incident. It is not difficult to predict the type of questions that would be asked; formulating convincing responses might be more problematic. How can security officers demonstrate that they take all reasonable efforts, to optimally deploy security resources?

Accountants have long since recognised that their professional competence may be demonstrated by a pristine set of financial records. An accountant will probably give a high priority to the maintenance of such records, when accepting a new appointment. Hence accountancy students are taught bookkeeping in their first year, however, few information security courses and textbooks provide an insight in the development and maintenance of information security documentation.

It is suggested that a comprehensive set of security documentation can serve to guide the security officer to an optimal information security stance, and to provide convincing evidence that a reasonable standard of professional competence had been maintained.
Security documentation can, inter alia:

- Document all significant policies pertinent to information security;
- Provide details of all systems and environments for which the officer has security responsibilities;
- Specify the security officer's responsibilities as formulated by senior management;
- Specify the degree to which some of those responsibilities have been delegated;
- Document the security systems and procedures developed in response to those responsibilities;
- Provide clear pointers to security logs and records, and reporting/ archiving responsibilities;
- Record the outcomes and subsequent actions, following risk analysis and security audits;
- Facilitate the design of security systems for new and enhanced IT systems;
- Facilitate audit and compliance exercises; and
- Provide senior management with an overview of the organisation's security stance.

The security officer should give careful consideration to the development and continual maintenance of an appropriate set of security documentation. Having said that leads to the obvious follow up question - how? The standards security topics, and implicitly encourage a top-down approach to security management, but they do not explicitly advise the security manager on the development of security documentation. Indeed, one of the significant dangers of the standards is that they will encourage the formation of security documentation, which serves to facilitate compliance audits, but does little to enhance organizational I.T. security.

In this paper, the role of security documentation is discussed and some suggestions are provided on the development of electronic documentation to facilitate information security management.
The range of meanings of documentation has been broadened and used to include the following:

(i) a collection of documents
(ii) a list of documents
(iii) a field of activity
(iv) a domain of science

or knowledge which sets theoretical bases of documentation activity, its methodology and techniques.

Technical Documentation

This means a collection of materials pertaining to a concrete technical activity, for instance, a collection of designs, drawings and estimates connected with construction of a defined structure.

A collection of documents kept in registries, libraries, archives and museums are exhibits which constitute documentation.

Documentation also includes a list of documents which embraces various catalogues and bibliographies, listing items of a defined collection of documents, "actual" and "ideal".

Documentation can be further described as the art involving activities comprising of document production, document distribution and document utilization.

DEFINITION OF DOCUMENTATION

1. "The science of ordered presentation and preservation of the records of knowledge, serving to render their contents available for rapid reference and correlation".
2. "The procedure by which the accumulated store of learning is made available for the further advancement of knowledge".
3. "The act of facilitation of the use of recorded, specialised knowledge through its presentation, reproduction publication, dissemination, collection, storage subject analysis, organisation and retrieval".

E.I. SHAMURIN defines documentation as collection, storage, organisation and bibliographical presentation of various kinds of documents facilitating their retrieval for scientific and information purposes.

It is described as a complex activity aiming at assigning various documents to a given problem and dissemination of such documents on the said problem as well as dissemination of information on these documents. The component activities are:

(1) Collection of documents
(2) Their documentation as presentation.
(3) Dissemination of Information on documents.
(4) Information service.

Documentation, then is concerned with the theory and practice of producing storable items of information in a form of convenience to the user, and so organizing them as to facilitate their retrieval and dissemination.

FUNCTIONS OF DOCUMENTATION CENTRES/REGISTRIES

The functions of Information Services are:

1. to provide scientists and experts in various fields with all necessary information pertaining to their problems.
2. to provide information on new facts which emerge in a given field.

The performance of these functions and the efficiency of the operation of information service depend on adequate organisation and on the selection of proper forms and methods of work, adapted to the needs of a determined category of recipients (users) of information and to the responsibilities laid on information. The complexity of these activities consists of a variety of operation performed by Information, documentation. Centres and Registries as well as Libraries.

These centres/posts constitute organizationally independent units or more commonly, they operate within the framework of various institutions, enterprises, offices, various organisations etc. A characteristic feature is their strictly determined specialization and activity aimed at provision of information from a defined field to a defined circle of recipients.

COLLECTING OF SOURCES OF INFORMATION

The basic function of documentation and information centres is the selection of collections of documents which constitute sources of information. Such functions can be performed by a library or registries which either forms a part of a documentation center or is a separate organisational unit within the framework of a given institution. Often enough, particularly in smaller documentation and information centres, the library/ documentation centre does not constitute a separate unit.

The object of collecting documents in centers of documentation and information is, above all, their utilisation for the elaboration of appropriate information material and the most rapid possible provision original documents. In the exact and natural sciences, in technology, in industry, in economics and in other fields of practical activity, only the 'tow and latest publications are used, the older being seldom sought for.

This is why some documentation centres after a lapse of time eliminate from their collection certain outdated documents.

Types and forms of documents collected by documentation and information centres are

highly diversified and their selection depends on the specificity of individual fields and on the needs of various groups of users.

Current periodicals reflecting the present state of knowledge in a given field, constitute the most important category of documents. Consequently, this group of publications belongs to the basic sources of information collected.

But for the exact and technical sciences, particularly in spheres in which the progress is very rapid as for instance nuclear physics or electronics periodicals are already becoming much too slow an instrument of information.

Here, the primary role is played by research reports often unpublished which are the first to present results achieved in laboratories of research workers.

For technology, industry and other fields of economy of great importance are patents, standards and what is called "factory documentation", industrial catalogues, prospectives, price list, description of machines, appliances and apparatus. Information posts in production enterprises collect documents which are related to the activity of the parent enterprises: plans, reports, instructions, and descriptions of production processes.

In addition to printed or mimeographed documents, also included in documentation collections are typed scripts and manuscripts, technical drawings, diagrams, statistical tables, maps, plans, sheet music illustrations, posters, placards etc.

Documentation centres prepare microfilms as a part of their collections; this is dictated by various reasons.

A separate group of documents collected by documentation centres constitutes what is called VISUAL OR AUDIO-VISUAL DOCUMENTS. This term embraces documents containing a fixed record of an image and sound, which is transmitted to the user by means of a special apparatus.

In this category are slides and silent films, phonograph records and sound tapes with a verbal or musical text, and sound films.

Finally, mention should be made of a special group of documents, comprising various kinds of objects, collected by certain documentation centres and which serve as subjects of investigation or as models of definite things. These can be exhibits from natural history collections of minerals, plants, insects, animals etc. Objects of art, industry, appliances and apparatus, models and dummies of such are also examples of such exhibits.

Not every documentation centre, of course, collects all the kinds and types of documents mentioned. Their selection depends on the specialization of individual centres, on their functions and their aims.

SECURITY DOCUMENTATION: Nature and Scope

The potential applications of information security documentation were listed above and this list provides an insight into the proposed set of documentation. Since we are dealing with information security in a complex and dynamic IT environment, the documentation should clearly be maintained in electronic form, with databases employed for all items comprising significant amounts of detail, and html linkages between relevant sections.

The security documentation could be considered from the following perspectives:

- Policies,
- Information Assets,
- Systems and Environments,
- Responsibilities,
- Security Systems and Procedures,
- Records, Reporting and Archiving,
- Security Audits and Business Continuity Planning,
- System Development, and
- Compliance.

POLICIES ON SECURITY DOCUMENTATION

Policies

Organisational security policies commonly come in one of three varieties - the non-

existent, the bland and the treatise on passwords. The security officer is well advised to explore and document all the implicit and explicit organizational policies, which could have some impact upon information security. These policies may then be used to establish the various aspects of the organisation's information security policy.

Organisations will have, at least implicit policies to ensure their continued existence, by abiding with all legislative, regulatory and contractual requirements. Such requirements commonly have implications for the integrity, availability and often confidentiality, of certain records and hence on security requirements.
The assets and finances of an organization are subject to control and recording policies: authorizations, four eyes' principles, segregation of duties, audit trails etc. As such manual processes migrate to IT systems, these policies also remain as significant security requirements.

Some policy areas may have more subtle impacts upon information security. The deleterious effects of offensive email, in a climate increasing sensitivity to harassment and discrimination issues, were easily predicted. Nevertheless, some organisations still lack systems and procedures to respond to such misuse of information systems. Similarly social concerns may lead to demands for accessibility to certain organizational information, or for dial up access for classes of disadvantaged employees, with attendant network security implications.

The part of Privacy Policy that is related to the protection of personal data will clearly have implications to information security. The current and emerging laws on intellectual property will also be a major concern, particularly in terms of installed software and material downloaded from the Web.

Personnel policies and related outsourcing issues will have less subtle impacts upon information security, particularly if they produce a high level of mobility amongst privileged information system users, or contract out IT processing without strict contractual requirements on information security.

The information security officer would thus be well advised to hold documentation on all relevant management policies, to consider them and to report upon their implications for the organisational security policy.

Information Assets and Security Documentation

The security officer is responsible for the protection of the information assets, but what are these assets and what degrees of priority are given to them? The problem of assigning dollar values to electronic files was recognised in the days of Courtney Risk Analysis [1], and the current problem is much more complex than that. The questions faced by the security officer are, inter alia, *what is the business impact arising from the*:

- Loss of confidentiality of this data item
- Loss of integrity of this data item;
- Unauthorised invocation of this transaction; and
- Loss of availability of this business process for this specified period of time.

Even the development of an inventory of the total set of data assets is a task ranging from the mammoth to the impossible. Nevertheless, the security officer should at least document classes of data and business processes, together with a mapping to the systems storing, processing and transmitting those classes and if possible, an impact rating of the classes. Given the draconian laws arising on intellectual property, the security officer will need to maintain a register of all installed software and license agreements.

Systems and Environments of Security Documentation

It is self-evident that the security officer should document the relevant details of all lT systems, buildings etc. within their aegis. The problem is to ensure that this documentation is continually updated in current networked environments. Ideally the IT departments would supply this information electronically and security officers then merely require a

linkage from this documentation. In such a case, is there some mechanism by which the security officer can highlight recent actual or proposed changes so that the security implications can be considered?

At the other end of the spectrum, the production and maintenance of this aspect of the documentation may be extremely time consuming. Such a situation is one requiring urgent attention, since it implies that the security officers are not adequately informed of the systems and environments they are required to protect.

Responsibilities of Security Documentation Manager

No security system is 100% effective and security officers commonly complain of a lack of support from senior management. In these circumstances security officers cannot guarantee that security incidents never arise and they will implicitly bear some degree of responsibility for any consequent business impacts. Hence the security officers would be wise to obtain a full statement of their own responsibilities, and develop an organisational chart showing the explicit delegation of those responsibilities.

The security officer should also be in a position to call upon a full description of the security responsibilities of all employees, contractors etc. In the event of a security incident this documentation should be able to highlight either:

- The individuals that failed to meet their security responsibilities, or
- Inadequate, or unrealistic, specification of security responsibilities.

Delegation of security responsibilities also implies a commitment to ensure that such delegations are not unreasonable in terms of the expectations placed upon employees. Hence, this set of documentation should also contain full details of the proposed and actual systems for security training, with links to training material, course details, staff attendances etc.

Security Systems and Procedures of Security Documentation

The documentation must clearly contain details of security systems, e.g. firewalls, VPNs, swipe card access control, virus protection software, authentication servers etc. and associated procedures, e.g. allocation of access privileges and passwords, much of this material is commonly embedded in other documentation and, in the first instance, a comprehensive set of linkages should be established.

The security officer clearly needs to have access to such details of security systems and procedures in the first instance. However, this section of the documentation also provides an insight into the role of the security officer, because it raises a number of significant questions:

- How do these security systems and procedures correlate with the systems and environments documentation (See 2.4)?
- What are the roles of these security systems and procedures, i.e. what assets are they protecting against what threats?
- What are the threats and assets that are not covered by these systems and procedures?
- Are the strongest security systems and procedures directed to the highest areas of risk?
- What is the degree of effectiveness of the systems and procedures prioritized in order of risk?
- Do any of these systems and procedures represent, in themselves, single points of failure?
- Are these systems and procedures themselves vulnerable to attack?

Clearly these questions cannot be answered by an inventory of security systems and procedures. Such a discussion involves the complex linkages between all the entities involved a risk analysis, threats, systems (physical and logical), vulnerabilities, security systems, information assets and the organisational reliance upon those assets. The security officer requires an effective active

security model to tackle these questions (See 3). A security officer would do well to reflect that the questions posed above could well be asked by a hostile barrister, in legal case following security incident that caused financial loss to other parties.

Records, Reporting and Archiving of Security Documentation

Senior management, legal and law enforcement advice is essential, to develop a full understanding of the security officer's responsibilities in protecting and/or maintaining:

- Organisational reports and archives as required by senior management policy, regulatory or legislative bodies; and
- Operating and security logs and reports.

This section of the security documentation should contain details of those set of data, e.g. tax return information, essential to ensure organizational compliance with contractual, legal, regulatory or legislative requirements.

Linkages or cross references to other sections of the security documentation are also recommended e.g.

- Systems and environments: Where are the records stored and processed?
- Responsibilities: Who are responsible for their security?
- Security systems and procedures: What are the security provisions for their protection?
- Security audits: Were any recommendations made for their protection and what subsequent action was taken?

The operating and security logs and reports are clearly of vital importance. This set of documentation should be headed by all relevant advice, from legal and law enforcement agencies, on the collection, handling and retention of such data, particularly in respect of data that may be used in legal proceedings.

In addition to the security reports and logs themselves, this section must contain all relevant supporting documentation to ensure that the reports and logs can at some later date be fully exploited in investigations and if necessary, submitted in legal proceedings. Linkages and cross references to other documentation will include, inter alia:

- Systems and environments to ensure that details as of the date that the records were taken are available; and
- Responsibilities particularly in relation to capturing security data.

Security Audits and Business Continuity Planning

A comprehensive set of security documentation will greatly facilitate security audits, and security audit reports etc. can themselves be a valuable component of security documentation. Such reports will normally provide an overview of the security situation at the time of the audit and a series of recommendations.

The security officer should document not only the reports but also the follow up actions to the recommendations; including a follow- up schedule, showing the progress of implementation and also reasons for delayed or non-implementation. There is ample material available on the documentation of Business Continuity Planning and it is suggested that such documentation may also be maintained in this section, with appropriate linkages to the other sections.

System Development of Security Documentation

In many cases security officers have responsibility for protecting systems that were not designed with a high priority given to security. Hence it is important that a security officer provides well-documented and reasoned cases for security implementation in new or upgraded systems. In the cases of system modification or upgrade the security officer needs to give careful consideration to:

- The risks of the current system;
- The security, and security rationale, provided against those risks;
- The risks of the proposed system;

- Proposed removal of any erstwhile security systems or procedures; and
- The security and security rationale to be provided against the risks of the proposed system.

If the risks, security and security rationale of the erstwhile system were adequately documented, then this exercise is greatly facilitated. If such documentation is not available, then there is a significant danger that system changes will introduce new risks, or remove undocumented but important security systems or procedures of the original system.

Compliance

This section of the documentation should provide an overview of the security stance of the organisation and highlight any major areas of concern by cross linkages, e.g. management policies that are not being met by current security systems and practices, security audit recommendations still outstanding, inadequate security logging in case of a security incident etc.

In this section the security officer would be wise to make a detailed list of security recommendations for senior management and record them for that interview with the hostile barrister.

SECURITY MODEL AND DOCUMENTATION

One of the major problems with most security documentation is that it is commonly embedded in documentation intended for another purpose, e.g. Operating Manuals, System Design Reports etc. Documentation intended primarily for security purposes tends to be addressed at a macro level, e.g. standards, risk analysis report. Information at this level tends to focus on what security is to be achieved rather than how to achieve it. Rarely does one read current documentation and feel that it gives a genuine insight into the security stance of an organisational system, i.e. it is often difficult to answer the major questions of the security officer: Where do I need to focus attention, what are the priorities for the future?

The Risk Data Repository (RDR) [24] was developed some years ago as a risk analysis model and during this work, it became clear that the RDR also provided an insight into the requirements for security documentation. A prototype system was developed in Visual Basic and current work is directed to developments, which could make more effective use of PC browsers to handle the linkages amongst the entities. It also clear that the early RDR did not adequately address the role of networks.

Nevertheless, the RDR described entities in terms of their roles from a security viewpoint, demonstrated the security inter-relationships of those entities and facilitated the computation of risk parameters. The entities of the earlier model are being replaced with a greater emphasis on networks and countermeasures. It is suggested that this model provides a basis for security documentation in electronic form that can:

- Be easily updated in rapidly evolving environments; and
- Facilitate the extraction of security information for various purposes, e.g. risk analysis, security design etc.

Structure of Security Entities

In the discussion on documentation above, it was suggested that the security officer should maintain documentation on *Information Assets*; Systems and *Environments; Security Systems and Procedures; and System Development.* It was also noted that it would normally be quite difficult to extract the information required by the security officer from current documentation.

It is suggested that a security model could provide a means by which a security officer records the relevant security information and gradually builds up application packages to assist in the analysis of that information. In the first instance, the entities of the model are defined, followed by the security linkages for such entities. The proposed entities relate the physical and logical aspects of security. At the top end of the model, the Information Assets are processed by Application Systems, which

in turn are hosted by Virtual Networks. These Virtual Networks are in turn hosted by Physical Networks. The Physical Networks comprise a set of interconnected units and are located in Physical Platforms, which themselves are located in a Physical Environment.

The purpose of the model is to highlight the security inter-relationships between the entities in a manner that facilitates the task of the security officer. The major entities included in the model are:

- A Unit - individual item of equipment + plus its accessories. Unit come in four categories End User (EU), Server (SU), Sensitive Data Storage Unit (SDSU) and Coms (CU) (NB cabling and wireless is considered as a Coms Unit).
- A PHYSICAL NETWORK (PN) - a collection of interconnected Units, one or more of which is a cabling or wireless Unit.
- A PHYSICAL PLATFORM (PP) - a collection of standalone Units and all SDSUs and physical networks located in a physical area.
- A PHYSICAL ENVIRONMENT - a collection of sites and buildings with associated essential services and physical security functions that hosts Physical Platforms.
- A VIRTUAL NETWORK (VN) - one or more physical networks, with common security architecture and / or a grouping associated with an AS.
- AN APPLICATION SYSTEM (AS) - one or more virtual networks used to host an information processing and/or communication application.
- INFORMATION ASSETS (IA) - data and processes, which, if attacked, could cause significant harm to the organization.
- INTRINSIC THREATS (IT) - those events that may cause harm to information assets and whose occurrence cannot be prevented, e.g. environmental threats (fire, extreme weather conditions), personnel physical (damage or misuse of equipment) and personnel logical (attacks mounted over networks etc.).

These entities have however, been chosen so that the linkages between them provide security officers with an insight into the security of their systems. These linkages are described in the next section.

Inter-relationships of Security Entities

The security entities described in the previous section are inter-related from a security viewpoint. The emphasis is now on the physical network, as the logical grouping of equipment items. If a building (Physical Environment) hosting a Physical Platform is damaged by some intrinsic threat event, e.g. fire, the security officer will be more interested in the effect upon a Physical Network than an individual item of equipment. Any standalone items will be separately linked to the Physical Platform and to the Application System. The security entities facilitate the tracing of threat events to their ultimate consequence, which is a business impact. If the model is recorded as an electronic document, with html links, then the security officer can easily postulate a number of potential intrinsic threats and then trace their likely paths to determine the ultimate business impact. The threats may be classified as:

- Environmental (e.g. flooding), impacting upon Physical Environments,
- Personnel Physical (e.g. attacker enters secure area containing an SDSU), impacting upon Physical Platforms, and
- Personnel Logical (e.g. attacker gaining access to sensitive server over a network), impacting upon Virtual Networks.

Having traced an attack, the security officer will then be concerned with the degree to which the security measures mitigate such an attack. In this model, it is suggested that such security measures can be effectively represented as Threat Countermeasure Diagrams [5]. In this approach, each countermeasure is considered to counter the incident threat but also to introduce consequent threats arising from loopholes in

the countermeasure or attacks on the countermeasure itself. Supporting countermeasures are commonly employed to address these consequent threats and a Threat Countermeasure Diagram is an effective means of representing such countermeasure rationale.

Role of Information Security Documentation

Support for Risk Assessment

The information security industry has made significant advances to meet the perceived threats to organisational information security. Originally, outside the military sector, the major threat identified by the finance and banking industry was the security of electronic transactions and security manufacturers supplied hardware cryptographic systems to this market. The advent of viruses in the late 1980s spurred a new industry in anti-viral software. Later, the development of the Internet as a common communication channel for organisations, expanded the hacker community and the production of firewalls to thwart them. PKI companies provided cryptographic software the emerging E-commerce market and many organisations now invest in various access tokens such as smart and magnetic stripe cards. The biotechnology industry is also continually gearing itself up for its promised future.

Nevertheless, security officers can face a difficult task in convincing management that these vendor products represent only a part of the solution. Individual countermeasures must be embedded within a coherent information security infrastructure, if the organisational operations are to be adequately protected. The development of such an infrastructure must itself be guided by effective risk assessment projects. The importance of effective risk analysis was recognised in the early 1970s [8] and there was a strong move by some governments to facilitate the adoption of such methodologies in sensitive computing systems.

Risk analysis includes the identification of assets, threats, vulnerabilities, countermeasures and the evaluation of loss expectancy. An information security risk analysis study defines the IT environment under consideration and recommends corrective actions.

Risk analysis projects were relatively expensive, even in the mainframe computing era, because they involve the collection and evaluation of a significant volume of data including the intrinsic threats, the IT system, its physical and operating environment, the assets to be protected and the business functions dependent on those assets.

Such risk studies were either conducted by in-house staff or external consultants. In general, the in-house staff often lacked extensive experience of the subjective aspects of risk evaluation and consultants had no previous knowledge or experience of the organisational system under study. Generally, the existing documentation was inadequate, in terms of its content, detail and currency, for risk assessment. Hence, the initial familiarization process was normally accompanied with a major task of data collection.

The magnitude of this initial familiarization task escalated rapidly, as systems evolved from batch processing mainframes to current complex, multisite networked, client server scenarios. Moreover, the batch processing mainframe environment was stable for long periods, usually between purchases of the mainframe equipment. Hence risk assessment recommendations had a long half-life, significantly reducing the average annual cost of such studies.

Security Documentation Requirements

It is much easier to make a case for the development of comprehensive security documentation, that to actually produce the documentation itself. In many cases, advice takes the form “I would not start from here”.

The information security management standards do provide an infrastructure for information security management, which at least suggests a structure for the documentation. A recent paper by the authors [6] suggested the type of current

organisational documentation and data that should be collected and packaged to form an initial set of information security documentation.

In this paper the necessary facets of security documentation are described and some insight into recent work on an Information Security Model is discussed.

At the outset the question arises – what is being described by the security documentation? Most system documentation is designed to assist operators and developers in the performance of their tasks. Security documentation is not however aimed at normal system operation, but rather at the circumstances in which the system fails, in some sense. Hence, security documentation should provide a detailed description of an agreed security model for the system. In other words, an organisation's security documentation should contain the local parameters of a generally accepted information security model.

The proposed model need not be described in conventional textual format. Given the complexity, magnitude and volatility of modern information systems, some form of database representation is more appropriate. Moreover, such a database should be supported with software tools and GUIs to facilitate the development, updating, investigation, risk analysis and security reporting.

If a common model were employed by organisations, then third party vendors would be encouraged develop support software. Moreover, given a common format of security documentation, one could envisage situations in which external security advice and expertise were readily absorbed by an organisation. Hence, it is possible to envisage a system in which CERT Advisories are automatically downloaded and added to the security database. The security software could then generate a report on the implications of the reported attack for the organisation.

REFERENCES

Akinade A. (2006) "Manual on Communication and Documentation Intelligence" ISN Publications, Lagos.

Akinade A. (2004) "Manual on Communication and Documentation Intelligence" ISN Publication Series, Lagos.

Courtney, R.H. JR., "Security risk assessment in electronic data processing systems." AFIPS Conference Proceedings 1977, pp.97104.

Anderson, A.M., Longley, D., and Tickle, A.B., "The Risk Data Repository: A Novel Approach to Security Risk Modelling".

Computer Security, Proc. IFIP TC 11 9th Int. Conf. on Information Security (Editor Dougall), IFIP Sec.'93, Toronto, Canada, 12-14 May 1993, NY: Elsevier Science Publishers, 1993, 185-190.

Anderson A, Kwok L F and Longley D, "Security Modelling for Organisations", Proc. of 2nd ACM Conf on Computer and Communication Security, Fairfax Virginia, USA, 2-4 Nov 1994, pp.241-250.

Kwok L F and Longley D, "A Security Officers' Workbench", Computers and Security, Vol.15, No. 8, 1996, 695-705.

Caelli, W., Longley, D., and Tickle, A.B. "A Methodology for Describing Information and Physical Security Architectures". IT Security: The Need for International Cooperation, Proc. IFIP TC11

8th Int. Conf. on Information Security (Editors Gable and Caelli), IFIP Sec.'92, Singapore, 27-29 May 1992, NY: Elsevier Science Publishers, 1992, 277-296.

Kwok, L.F. (1997): A hypertext information security model for organizations, Information Management and Computer Security, Vol. 5 No.4, pp 138-48.

Anderson AM, Longley D and Kwok LF (1994): Security Modeling for Organizations, Proc. 2nd ACM Conf on Computer and Communications Security, Fairfax VA, pp. 241-250.

IT Baseline Protection Manual Standard Security Safeguards, URL:http://www.bsi.bund.de/english/index.htm

British Standards Institute (1999), BS7799: 1999 Information security management, Part 1 Code of practice for information security management, Specification for information security management systems.

SECURITY EDUCATIONAL TRAINING AND MANPOWER DEVELOPMENT

A SYTEMATIC REVIEW OF SAFEGUARDING STUDENTS IN THE UNIVERSITY SYSTEM

Adebiyi, Deborah Toyin & Olusakin, Ayoka Mopelola.

Abstract

Safeguarding is yet to be prioritized in research in Africa despite the level of its indispensability. Students in Nigeria universities are faced with a lot of safeguarding challenges that are yet to be fully addressed. The challenges range from insecurity in form of kidnapping or abduction; raping, drug abuse, yahoo/yahoo(duping) ritual killing and victimization among others. A literature search was conducted to identify studies on safeguarding. Systematic review of UK research and policy was used to gain insight to a contemporary picture of safeguarding issues and practice. This study is therefore set out to highlight a systematic review of safeguarding in university system. The following recommendations are suggested: there should be provision for Safeguarding framework to advance protection and safeguarding of the university system. Policy and practice that will safeguard the vulnerable university students, staff and visitors to the university, among others, should be embarked on.

KEYWORDS: Abuse, Harms, Protection, Safeguarding, Vulnerable

INTRODUCTION

What is Safeguarding?

Basically, safeguarding in the university system is a process of ensuring that vulnerable university staff, students as well as visitors to the university, are protected from neglect, abuse or exploitation. Safeguarding is not limited to students' protection but it is all encompassing. Though safeguarding and protection are often used interchangeable, protection is about students being protected from risk of abuse while safeguarding involves protection of the best interest of each student from significant harm. This includes protection from abuse, harm to health or development, necessary care that match the needs of the university students and ensure the best possible results. Safeguarding of students is mainly concerned with provision of safe environment and creation of awareness on availability of help when needed. University Safeguarding Centre should be able to handle safeguarding issues in conjunction with the university Security Unit, Medical Centre, Students Affairs, Counselling Unit and all stakeholders. Safeguarding is to take all necessary steps to prevent harm, abuse, sexual exploitation and harassment of any sort from occurring. Protection of people especially university students and staff, from harm and be at alert to respond to emergencies promptly when there is an occurrence of such. In addition, safeguarding is for people who, because of issues such as dementia, learning disability, mental ill-health or substance abuse, have care and support needs that may make them more vulnerable to abuse or neglect.

It requires proactively identifying, preventing and guarding against all risks of harm, exploitation and abuse and having mature, accountable and transparent systems for response, reporting and learning when risks occur. Those systems must be survivor-centered and also secure those accused until an investigation is completed.

Historical background of Safeguarding

Safeguarding Children:

Child protection has gone through many changes over the past century, re-defining its objectives as our understanding of abuse has changed. Now it includes not only neglect, economic exploitation, and cruelty, but emotional, psychological, and sexual abuse as well.

So, child protection enters the 21st century with a substantial depth of good – but often painful - experience of welfare and law. It mostly attracts people of integrity, with a love of children and justice, people with wisdom, patience and vision, able and willing to work

within the statutory framework. Ambode (2016) in Lagos state safeguarding and child protection policy clarified safeguarding as a term which is broader than 'child protection' and relates to the action taken to promote the welfare of children and protect them from harm. Safeguarding is protecting children from maltreatment; preventing impairment of children's health and development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; taking action to enable all children to have the best outcomes.

According to Barbara (2019) in the history of child protection stated that a generation passed before the next piece of legislation, the 1932 Children's and Young Person's Act reminded society that there were children still at risk. The Act's main aim was to establish working conditions for young people leaving school as well as for those still at school (university students inclusive) and working part-time.

Why safeguarding in the university system?

Insecurity challenges in Nigeria have affected teaching, research, community services programmes of higher education in Nigeria. Rising level of insecurity have also birthed a reduction in the investment in higher education, led to death of some students, academic and non-academic staff and the destruction of infrastructural facilities in Nigeria (Ogunode, Ukozor & Ayoko, 2023).

In his opinion Matthews (2008) emphasized the need to detect abuse and neglect at an early stage to protect the child and enable the provision of assistance to the child, the parents and family "The University also has a duty of care to its staff, students and visitors and is responsible for ensuring appropriate policy, procedures, guidance, risk assessment, action planning and training are in place to facilitate effective safeguarding of children, young people and adults at risk. This includes ensuring we take reasonable steps to ensure that contractors understand, accept and are responsible for their, or their employees' conduct in connection with these groups on university premises" Universities are accountable for creating a safe learning environment on campus and extenuating "foreseeable" threats.

What are the ten different types of abuse?

Social Care Institute for Excellence, UK, (SCIE) (2020). In the Care and support statutory guidance identifies ten types of abuse, these are:

Physical abuse

Types of physical abuse

- Assault, hitting, slapping, punching, kicking, hair-pulling, biting, pushing
- Rough handling
- Scalding and burning
- Physical punishments
- Inappropriate or unlawful use of restraint
- Making someone purposefully uncomfortable (e.g. opening a window and removing blankets)
- Involuntary isolation or confinement
- Misuse of medication (e.g. over-sedation)
- Forcible feeding or withholding food
- Unauthorised restraint, restricting movement (e.g. tying someone to a chair)

Domestic violence or abuse

Types of domestic violence or abuse

Domestic violence or abuse can be characterized by any of the indicators of abuse outlined in this briefing relating to:

- Psychological
- Physical
- Sexual
- Financial
- Emotional.

Sexual Abuse

Types of sexual abuse

- Rape, attempted rape or assault
- Inappropriate touch anywhere
- Non- consensual masturbation of either or both persons
- Non- consensual sexual penetration or attempted penetration of the vagina, anus or mouth
- Any sexual activity that the person lacks the capacity to consent to
- Inappropriate looking, sexual teasing or innuendo or sexual harassment

- Sexual photography or forced use of pornography or witnessing of sexual acts
- Indecent exposure

Psychological or Emotional Abuse
Types of Psychological or Emotional abuse

- Enforced social isolation – preventing someone accessing services, educational and social opportunities and seeing friends
- Removing mobility or communication aids or intentionally leaving someone unattended when they need assistance
- Preventing someone from meeting their religious and cultural needs
- Preventing the expression of choice and opinion
- Failure to respect privacy
- Preventing stimulation, meaningful occupation or activities
- Intimidation, coercion, harassment, use of threats, humiliation, bullying, swearing or verbal abuse
- Addressing a person in a patronizing or infantilizing way
- Threats of harm or abandonment
- Cyber bullying

Financial or Material Abuse
Types of Financial or Material Abuse

- Theft of money or possessions
- Fraud, scamming
- Preventing a person from accessing their own money, benefits or assets
- Employees taking a loan from a person using the service
- Undue pressure, duress, threat or undue influence put on the person in connection with loans, wills, property, inheritance or financial transactions
- Arranging less care than is needed to save money to maximize inheritance
- Denying assistance to manage/monitor financial affairs
- Denying assistance to access benefits
- Misuse of personal allowance in a care home
- Misuse of benefits or direct payments in a family home
- Someone moving into a person's home and living rent free without agreement or under duress
- False representation, using another person's bank account, cards or documents
- Exploitation of a person's money or assets, e.g. unauthorised use of a car
- Misuse of a power of attorney or other legal authority
- Rogue trading – e.g., unnecessary or overpriced property repairs and failure to carry out agreed repairs or poor workmanship

Modern Slavery
Types of Modern Slavery

- Human trafficking
- Forced labour
- Domestic servitude
- Sexual exploitation, such as escort work, prostitution and pornography
- Debt bondage – being forced to work to pay off debts that realistically they never will be able to

Discriminatory Abuse
Types of Discriminatory Abuse

- Unequal treatment based on age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex or sexual orientation (known as 'protected characteristics' under the Equality Act 2010)
- Verbal abuse, derogatory remarks or inappropriate use of language related to a protected characteristic
- Denying access to communication aids, not allowing access to an interpreter, signer or lip-reader
- Harassment or deliberate exclusion on the grounds of a protected characteristic
- Denying basic rights to healthcare, education, employment and criminal justice relating to a protected characteristic
- Substandard service provision relating to a protected characteristic

Organisational or Institutional Abuse
Types of Organisational or Institutional Abuse

- Discouraging visits or the involvement of relatives or friends
- Run-down or overcrowded establishment
- Authoritarian management or rigid regimes
- Lack of leadership and supervision
- Insufficient staff or high turnover resulting in poor quality care
- Abusive and disrespectful attitudes towards people using the service
- Inappropriate use of restraints
- Lack of respect for dignity and privacy
- Failure to manage residents with abusive behaviour
- Not providing adequate food and drink, or assistance with eating
- Not offering choice or promoting independence
- Misuse of medication
- Failure to provide care with dentures, spectacles or hearing aids
- Not taking account of individuals' cultural, religious or ethnic needs
- Failure to respond to abuse appropriately
- Interference with personal correspondence or communication
- Failure to respond to complaints

Neglect or acts of omission
Types of neglect and acts of omission

- Failure to provide or allow access to food, shelter, clothing, heating, stimulation and activity, personal or medical care
- Providing care in a way that the person dislikes
- Failure to administer medication as prescribed
- Refusal of access to visitors
- Not taking account of individuals' cultural, religious or ethnic needs
- Not taking account of educational, social and recreational needs
- Ignoring or isolating the person
- Preventing the person from making their own decisions
- Preventing access to glasses, hearing aids, dentures, etc.
- Failure to ensure privacy and dignity

Self-neglect
Types of self-neglect

- Lack of self-care to an extent that it threatens personal health and safety
- Neglecting to care for one's personal hygiene, health or surroundings
- Inability to avoid self-harm
- Failure to seek help or access services to meet health and social care needs
- Inability or unwillingness to manage one's personal affairs

Six principles of safeguarding

First introduced by the Department of Health in 2011, but now embedded in the Care Act, these six principles apply to all health and care settings (SCIE, 2020).

1. **Empowerment**: People being supported and encouraged to make their own decisions and informed consent.

2. **Prevention**: It is better to take action before harm occurs.

3. **Proportionality**: The least intrusive response appropriate to the risk presented.

4. **Protection**: Support and representation for those in greatest need.

5. **Partnership**: Local solutions through services working with their communities. Communities have a part to play in preventing, detecting and reporting neglect and abuse.

6. **Accountability**: Accountability and transparency in safeguarding practice

Safeguarding framework

Contextual Safeguarding Coined by Firmin (2015), the term Contextual Safeguarding was first introduced in 2015 to provide a framework for ensuring child protection systems were equipped to respond to abuse that child – particularly adolescents - are

exposed to and/or experience in extra-familial settings. Initially, through a series of case reviews (Firmin, 2015, 2017a), and latterly through practice audits and action research in 14 local authorities in England (to develop responses to peer-on-peer abuse) (Firmin, et al., 2016; Lloyd, Fritz and Firmin, 2017), it became apparent that safeguarding partnerships required a framework that not only saw a child – and their behaviour 'in context', but was equipped to assess and intervene with those contexts when they were associated with risks and/or experiences of abuse. While research has long recognised that some forms of abuse that predominate in adolescence are associated more to community/peer contexts than familial ones (Barter, 2009b; Catch 22, 2013; Hanson & Holmes, 2015; Pain, 2006; Pitts, 2013; Sidebotham, et al., 2016), there has been little attempt to reform safeguarding practice in-line with this lived reality for children. Instead, relocation of adolescents away from schools and communities in which they have encountered harm, and Intervention that can build the resilience or change the behaviours of individual student who remain in harmful circumstances, have dominated the practice model – the role of social care and related safeguarding partners within this being the assessment of and intervention with families of adolescents affected by extra-familial risks or abuse – to better support (and in some cases control) their children (Firmin C, 2017a; Hanson & Holmes, 2015; Sidebotham, et al., 2016.

By critically examining this dynamic in partnership with practitioners, Firmin (2017b) developed a Contextual Safeguarding framework comprised of four domains to describe child protection approaches that would engage with extra-familial risk or abuse. These four domains posited that in order to sufficiently safeguard children – particularly adolescents – from risk or abuse in extra-familial settings, safeguarding partnerships need to:

a) **target** – the home, peer group, school, neighbourhood or online contexts where abuse occurs, through assessment and intervention, in addition to the individuals affected;

b) **do this within a child protection legislative framework** – to ensure that the response is welfare led, is not necessarily triggered by – or dependent upon – a crime being committed or a criminal investigation being conducted;

c) **build partnerships with agencies who have a reach into extra-familial contexts** – such as education, voluntary and community sector organisations, youth work, housing, retail, transport and licensing, in addition to children – particularly adolescents (as peers), and parents themselves: and

d) **measure success by risk reducing in contexts of concern** – not solely by a change in the behaviours of any individuals who have encountered or instigated abuse unsafe contexts.

Safeguarding would be relevant in:

- Providing Government departments, policy makers, local leaders, practitioners and others with positive insight to articulate what many already knew – at childhood age and also during adolescence, involvement in risks, harm or abuse could have negative impact on the concerned individuals, communities as well as the larger society.

- Stakeholders would also be equipped with vital information on students safeguarding framework through which to advance methods that are more reactive to hazards faced by and/or experiences of university students and their families.

Safeguarding systems and intervention

Prevention should be prioritized. In case of occurrence, early and proactive intervention should be involved. Studies in England that was carried out from 2013 to 2017 recommended:

Work with Fair Access Panels to explore the use of managed moves in response to vulnerability at school; the development of templates to collect information on peer-group dynamics as part of assessment processes, and; frameworks to contextualize multi-agency meetings about young people who had displayed harmful sexual behaviours. Since safeguarding risks could impact the emotional, physical and mental well-being of young people; drive their involvement in offending, using drugs and alcohol and going-missing; undermine their access to education and other services, and; negatively impact family relationships.

Safeguarding principles are critical for supporting young people to:

- recognize, and recover from, the aforementioned experiences; re-shape their constructive relationships; and re-involve in positive events.

- Students need to be supported to build protective peer relationships, within safe school and community settings.

RECOMMENDATIONS

- Need to establish safeguarding centres in all universities.
- Safeguarding should provide framework to advance protection and defense of university system.
- Policy and practice that will safeguard the university students and should be embarked on.
- Students and staff need to be supported to build protective peer relationships, within safe school and community settings.

References

Barter, C. (2009). In the Name of Love: Partner Abuse and Violence in Teenage Relationships. British *Journal of Social Work, 39,* 211–233.

Catch 22. (2013). The role of the family in facilitating gang membership, criminality and exit.London: Catch 22.Pain, R. (2006). Paranoid parenting? Rematerializing risk and fear for children. *Social and Cultural Geography, 7(2),* 221-243.

Equality Act 2010, c39. Available at https://www.legislation.gov.uk/ukpga/2010/15/contents

Firmin, C. (2015). *Peer on peer abuse: safeguarding implications of contextualising abuse between young people within social fields: Thesis.* Luton: University of Bedfordshire.

Firmin, C. (2017a). *Contextual Risk, Individualised Responses: An Assessment of Safeguarding Responses to Nine Cases of Peer-on-Peer Abuse*. Child Abuse Review. doi:10.1002/car

Firmin, C. (2017b) *Contextual Safeguarding: An Overview*. Luton: University of Bedfordshire.

Firmin, C., Wroe, L., & Lloyd, J. (2019). *Safeguarding and exploitation - complex,contextual and holistic approaches: Strategic Briefing. Dartington*: Research in Practice.

Hanson, E., & Holmes, D. (2015). The Difficult Age: Developing a more effective response to risk in adolescence. Darlington: Research in Practice.

Matthews,B. (2008) Protecting children from abuse and neglect. In Young, L & Monahan, G (Eds.) *Children and the Law in Australia. LexisNexis Butterworths, Australia, pp. 204-237.*

Ogunode, Ukozor & Ayoko, (2023). Insecurity Challenges and Higher Education in Nigeria. *Best journal of innovation in science, research and development Volume,2* Issue,5. ISSN: 2835-3579

Pitts, J. (2013). Drifting into Trouble: *Sexual Exploitation and Gang Affiliation*. In M. Melrose, & J.

Social Care Institute for Excellence, UK, (SCIE) (2020). Types and indicators of abuse. *At a glance 69.1*

Sidebotham, P., Brandon, M., Bailey, S., Belderson, P., Dodsworth, Garstang, J., Sore, P. (2016). *Pathways to harm, pathways to protection: a triennial analysis of serious case reviews 2011 to 2014:* Final report. London: DfE.

ETHICAL STANDARDS AND BEHAVIOURAL PATTERNS IN SECURITY AND LAW ENFORCEMENT

TOWARDS PROFESSIONALISM AND BEST PRACTICES IN SERVICE DELIVERY IN PRIVATE SECURITY INDUSTRY

Barrister Adebayo Akinade & Michael Adedotun Ojo

ABSTRACT

There is an ongoing need to make all employees in the company aware of the importance of the security function. Security employees should understand the importance of the security function and of their respective jobs. Induction sessions for new employees offer an opportunity for presentations by the Security Director or another representative of the department. Audio-visual materials such as slide/tape programs, Power Point presentations, audiotape, videotapes and motion picture can be used effectively. All newly hired middle-management personnel undergo an orientation session with the security Department. During this visit the new executive learns about the department's structure and function, meet the staff and tours the Security facility. Bulletins such as a security newsletter can be used to inform management of the Security Department's contributions to the company. Company meetings offer security representatives a chance to talk about their department's functions and answer questions. Security's relationship with other department can further be improved by involvement programmes that bring non-security personnel into contact with security.

INTRODUCTION

Security practice effectiveness and internal efficiency are central to the essence of security system. These are very crucial to security goal attainment as well as optimal resource utilization in organizations.

Effectiveness as used in this paper refers to the extent of overall goal attainment, while efficiency is related to the use of available resources frontal results. Professionalization in this context is defined and applied as a systematic co n ferment of dignified status on practitioners for obvious personal and public benefits.

The two concepts are frequently used to assess the performance of individual organizations. In usage, they have become almost inseparable as one is rarely used without the other. However, a closer look at their definition reveals their subtle differences for whilst "effectiveness" includes "efficiency", efficiency" does not necessarily include "effectiveness".

"Efficiency" and "Effectiveness" are two fundamental aspects of a successful administration, but what do they mean? Starting with the dictionary definition, efficiency (n) means "the state or quality of being efficient" and effectiveness (n) "the ability or power to have a noticeable or desired effect.

From here, a brief search was made into some literature and the following interpretations came up.

Koontz and Wehrich define Effectiveness as the achievement of organizational objectives and Efficiency as "the achievement of the ends with the least amount of resources. Drucker's definition is the most appealing he says Efficiency is "doing things right" and Effectiveness is "doing the right things". He adds that Effectiveness is the foundation of success whilst Efficiency is a minimum condition for survival after success has been achieved.

Effectiveness and Efficiency are vital to the essence of security practice in both private and public sectors. These concepts are very crucial for goal attainment as well as optimal resource utilization.

Effectiveness as used in this paper refers to the extent of overall goal attainment while efficiency is related to the use of available resources for optimal results.

Professionalization in this context is defined and applied as a systematic conferment of dignified status on practitioners for obvious personal and public benefits.

It is incontestable fact that every profession like Law, Medicine, Surveying and Architecture have both mainstreamed and "city side" practitioners.

The need for professionalization of security at all the various levels is hereby considered as a great weapon for high quality goal attainment in security practice in Nigeria.

The fact is that a professional status confers on the practitioners' notable benefits such as better public perception of the status of that profession to be higher than that of just a job. Studies of occupational prestige in a number of countries reveal that "while there are wide variations in prestige within the stratum, and even within specific occupations, the professions are accorded more prestige by the general public than any other occupational category.

Another benefit of professionalization to the job-holder is that of improved rewards deriving from the profession's higher degree of bargaining power. Furthermore, professionals control entry into the profession, limit entry as a form of social control which in turn leads to apparent scarcity and the attendant prestige. This bestows on them the power to apply the law of demand and supply.

PROFESSIONS, PROFESSIONALISM AND PROFESSIONALISATION

PROFESSION: The notion of "profession" can be traced to the early eighteenth century. Specifically in 171, Addison talked about "the three great professions of divinity, law and physics" (Carr-Sunders, 1966). Since then, many professions have evolved and many are evolving to this day. Notable professions in Nigeria today include Law, Medicine, Pharmacy, Engineering, Nursing, Architecture and Surveying. With each of these there exists subgroups that are also recognized. In Engineering, for example there are such subgroups as mechanical, civil and electrical/ electronic engineering.

By definition, "a profession is an ideal type of occupational institution with a limited number of occupations or vocations involving special learning which carries so much social prestige' Functionally, Benins defines it as "a calling based on a foundation of knowledge toward a clientele and with an ethical posture towards its clientele and members of the profession." This is in agreement with Carr-Saunders (1996) definition, which notes that a profession is "an occupation based upon specialized intellectual study and training, the purpose of which is to supply skilled service or advice to others for a definite fee or salary"

As With these occupations, can Industrial Security Practice in Nigeria be similarly accorded a professional status? To answer this question, one needs to consider the elements or the attributes of a profession, which can rightly be called professionalism.

PROFESSIONALISM

Professionalism simply refers to the ethos or expected standard of behaviour and performance of the "professionals". It includes: "the character, spirit and methods that distinguish a professional from an amateur. Professionalism is also viewed from two dimensions, namely; the structural and the attitudinal attributes.

(I) THE STRUCTURAL ATTRIBUTES

In terms of structural attributes, for a job or occupation to be accorded a professional status, the following must obtain.

(a) It must be a full-time occupation. The practitioner is "married" to the job as a lifelong career,

(b) There must be an established and duly accredited institution for the training of the members. That is why in Nigeria, there are the Nigerian Law School, Medical' Schools, Nigerian College of

Administration and Teacher Training Colleges, among others

(c) Every profession must have a professional association such as Nigerian Bar Association, Nigerian Medical Association, and Nigerian Society of Engineers and so on. Membership is dignifying, following special type of qualifications and license to practice the profession.

(d) Members must put in place a regulatory code of ethics, and these are invariably enforced by the professional associations.

(e) The professional body nurtures a clientele who has no choice but to accede to the professional judgement. In other words, clients are controlled by the profession's approved stipulations with logical orientation towards the practice and principles.

(II) THE ATTITUDINAL FEATURES

On the other hand, the attitudinal attributes of a profession comprise the following:

i. **Expertise**: The practice of a profession is rooted in a foundation of knowledge organized into an internally consistent function in the relevant body of knowledge.

ii. **Display of Authority**: deriving from the professional's expertise. This is variously known as "authority of competence", "authority of knowledge" or "sapiential authority". It is this unique authority that highlights the layman's comparative ignorance.

iii. **Self-Regulation**: Essentially, the professional does not subscribe to snoopy bossing, given the fact that he/she is a knowledgeable expert. He / She accepts collegial control. Basically, a professional must have the ability and willingness to make decisions without external pressures. He/her recourse is to the professional association or council as a major reference.

PROFESSIONALIZATION

Professionalization is process or movement towards professionalism. It is a progression from the periphery towards the idea type of occupation. The process of professionalization involves.

- Development of specialized skills and training such that the language of the profession sounds esoteric to the "uninitiated"';
- Establishment, through legislation, of minimum dues, fees and, or salaries;
- Formation of professional associations whose laws define labour relationships, career or occupational lives, individual and group-worth opinions and deep mastery of operating sentiments. That is quite distinct from labour/trade unions primarily concerned with members welfare and management of behaviour regarding workers and employees;
- Setting up a code of ethics for the members, emphasizing such conduct as standard of work, dedication, responsibility and emotional neutrality;
- Stipulate minimum qualifications for entrance into professional practice or activity;
- Enforcement or appropriate rules and norms (sanction) of conduct among member; and
- A conscious (planned) attempt to raise the status of the professional group in the large society aside the workplace prestige.

FUTURE DIRECTION OF PROFESSIONALISM IN PRIVATE SECURITY PRACTICE

As Ernest Greenwood (1966) says: "We must think of the occupation in a society as distributing themselves along a continuum". What this entails for us in Nigeria is that rather than write off Private Security Practice in the country, as a non-profession, we should all put our acts together to move it towards an appreciable level of professionalism. All the stakeholders under the aegis of the Professional Institute Association should be actively involved in the professionalization process. The following activities are recommended:

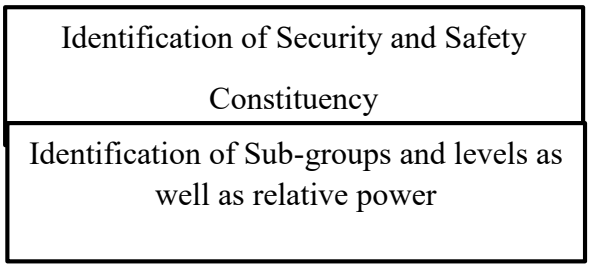
- Stipulating a Minimum Entry Qualification for Practice of security at various levels nationwide.
- Registration of Private Security Practitioners at the various tiers of the Security Systems Unregistered persons must not be allowed to practice at all.
- As it is done in other professionals, the Government in collaboration with the appropriate bodies should establish a distinct salary structure for the private practitioners in the public institutions.
- Proper definition of progression grades for members, stipulation of entry level, which will graduate into highest level with regulated retraining and professional development modules.
- The curriculum of security education should undergo a thorough review so as to make it relevant to the needs of a modern growing multicultural and pluralistic society as ours.
- Designing an integrated ethical code of conducts, a legal bond (by issuing members who passed board examinations/ licenses to practice), formed by personal and corporate values.

PROFESSIONALISING FOR SECURITY PRACTICE FOR EFFECTIVENESS, EFFICIENCY AND PRODUCTIVITY

For professionalization to impact favourably on overall effectiveness and internal efficiency, the following must be in place:

- A set of agreeable evaluation criteria;
- A clear perception of individual effectiveness even when the person is not in federal or state government service. This will throw more light on the task performance of the members as professionals;
- A heightened sense of dignity, physical gait and carriage, esteem, morale, motivation and conscientious of Nigerian Security Practitioners;
- Easy application of the systems model to attain educational effectiveness, involving a comprehensive search by the professionals themselves for their clients (threshold populations);
- Close interaction between Sub-groups and levels/types of security practitioners whose concern must revolve around their environment, personal/social and goals of Security system.

Professionalization of security practice should introduce a uniform code of conduct/ethics that will safeguard the strategic constituency of security and safety content, process and method. The following measures are to achieve the goals of security strategically using a body of professional:



It is noted that security vocation in both the public and private enterprises are usually criticized and almost receive condemnation though sometimes undeservedly for poor or no performance.

Despite the universality of security needs and the importance of the industry in the today's world, security practice is yet to become widely accepted as the complex and demanding profession it really is. The successful practice of security and safety as a

profession is contingent upon some related requirements, like in any other type of profession.

PRIVATE SECURITY: NEED FOR STATUS OF PROFESSIONALISM

There is no doubt that security at the macro-level qualifies as a profession. In the definition of macro-security, components of national security such as the Army, the Navy, the Air Force, the Police Force, the Customs and the Immigration were mentioned. In each of these enumerated security agencies, certain skills are required to accomplish the assigned roles. These skills are acquired through rigorous training. In addition to programmed rigorous training, members of each organization are required to observe certain laid down ethics.

In order to ensure strict compliance with the ethics of the profession, a body is put in place to regulate the activities of the organization. However, at the **micro-level of security**, this is not so. Micro-security, which is associated with individuals, the family, the community and corporate organizations, is yet to attain a professional status in Nigeria. Despite the fact that the operations of private guards are regulated by the **Private Guards Company Act 1986**, it is still very common to find quacks being employed as private guards.

Agreed that certain amount of skill and training are required of private guards, it is rather unfortunate that employers of private guards hardly attach much importance to the professional qualities expected of a guard. The implication of this negligence on the part of employers of private guards is obvious inefficiency with monumental consequences. In order to overcome problems associated with the employment of quacks as guards, some organizations and influential individuals have resorted to patronizing registered private security companies for trained and reliable guards. On the other hand, some organizations resort to maintaining their own proprietary internal guards in which recruitment, training, kitting, and remuneration are the responsibility of the organizations. The advantages of sourcing private guards from organized private security companies include:

a) The guards for security companies are given basic training.
b) Proper documentation of guards is carried out by the security companies,
c) The provision of uniform and other kits is the responsibility of the security companies.
d) The guards can easily be replaced at the request of clients.
e) It is economical because there is no payment of pension and gratuity.
f) Private security companies occasionally bear the liabilities arising from guards' inefficiency or negligence.
g) It dispenses with the involvement of guards in union activities.

In spite of the advantages of contract security guards, some organizations prefer to maintain their own internal security guards. The advantages of this system are:

a) Permanent internal guards tend to be more committed than contract guards.
b) Permanent internal guards do not have the problem of dual loyalty.
c) Command and control are very easy.
d) Easy mobilization for operations.
e) Administrative convenience.

There is need to attach proper attention to career progression and development as part of the processes of ensuring professionalism in the private security industry. Career progression and staff development is a broad administrative arrangement designed to ensure that the personnel is adequately prepared to perform its duties. This administrative arrangement is expected to deal with issues such as proper career structure, training, opportunity for promotion, welfare package, salaries, job security, etc.

In every organization, appropriate policies are expected to be formulated to take care of the above components of career progression and staff development. Under career structure, there is the need to ensure uniformity in the ranking of security staff in the industry. Qualifications and experience required of a staff member in each status must be spelt out, for example, the present system whereby every organization and institution adopts

different career structures for security staff is not good for professionalism.

Who is a Security, Safety and Protective Professional? A Security Professional is someone who is providing a service for the good of the public and private enterprises based on knowledge acquired by training and education leading to a demonstration of appreciable competence with utmost integrity and code of conduct of the Institute.

A Certified Security Professional denotes a person with the professional knowledge, skill, experience and personal qualities with the ability to manage security and protective resources art maximum effectiveness with least cost to ensure organizational efficiency and effectiveness.

WHAT TYPES OF SECURITY SERVICES ARE TO BE DELIVERED BY PRIVATE SECURITY PRACTITIONERS IN ORGANISATIONS AND COMMUNITIES?

Primary security operational services are those which are common to almost every community and organization.

The main services of security personnels in organizations are listed below:

Patrol Activities:

The conduct of preliminary investigations, continuing surveillance of hazards; provision of miscellaneous services to the public; crowd control; investigation of major and minor crime at the scene upon discovery or by request; enforcement of minor laws relating to vagrancy, begging, loitering, drunkenness, and other publicly offensive conduct; quelling disturbances of the peace; repressing disorderly conduct connected with personal, family and public disputes; attending to minor injuries and emergencies; the interview and interrogation of those persons who have given reasonable cause for suspicion of their guilt; issuance of warnings and citations; arrest of offenders; and continual observation of the community to determine the need for police intervention or assistance.

Investigatory and Intelligence Activities

Investigations of crime; recovery of stolen property arrest of suspended and identified criminals; and case preparations for prosecution. Among the more frequent crimes handled by these officers are criminal homicide (murder non-negligent manslaughter manslaughter by negligence); forcible rape; robbery (stealing or taking anything of value from the person or his presence by force or violence of by putting in fear, such as strong-arm robbery, stickups); aggravated assault (assault with intent to kill, assault by shooting, cutting, stabbing, maiming, poisoning, scalding or by use of acids); and burglary (breaking or entering, safe-cracking, or any unlawful entry to commit a felony or a theft).

Others are larceny (theft of bicycles, automobile accessories, shoplifting, pocket-picking, or any stealing or property or article of value which is not taken by force and violence or by fraud); auto theft (where a motor vehicle is stolen or driven away and abandoned); assault and battery forgery (counterfeiting, or making altering, uttering, or possessing, with intent to defraud, anything false which is made to appear true); embezzlement (fraud, con games, and obtaining money or property by false pretenses); stolen property offences (buying, receiving and possessing stolen property); weapons violation (disregard or regulation or statues controlling the carrying, using, possessing, furnishing, and manufacturing of deadly weapons or silencers); and offences against the family and children (non-support, neglect, dissertation, or abuse of family and children).

Vice Activities

The repression and control of those offences which tend to habituate and through habitation, tend to corrupt and destroy the physical, mental and moral health of the offender. Among the major vice areas are prostitution (sex offences of a commercialized nature, such as keeping a bawdy house, procuring, transporting, or detaining women for immoral purposes); sex offences (statutory rape, offences against common decency, morals and chastity such as sex perversion);

narcotics violations (offences relating to unlawful possession, sale, or use of narcotic drugs); liquor law violations (unlawful possession, sale, use of intoxicating beverages, selling liquor to minors, sales after illegal losing hours); gambling (promoting, permitting, or engaging in gambling).

Traffic Activities

The promotion of safety on the streets and highways; with particular reference to drivers and pedestrians. The major traffic responsibilities of security agencies centre around enforcement of the road and driving laws, including the drunk driving statutes; enforcement of parking ordinances; general enforcement of vehicle code requirements for vehicle code requirements for vehicles and vehicle operators; pedestrian control; investigation of traffic accidents; traffic direction traffic education; and to a certain degree, traffic engineering.

Crime Laboratory (Criminalistics) Activities

The provision of scientific and technical personnel and facilities for the analysis, identification and comparison of physical evidence. Ordinarily these services provide assistance in fingerprint operations (searching, developing, photographing, lifting, identifying, classifying and filling); offer advanced photographic service (developing, printing, and processing crime scene photographs, assisting in identification photography, providing specialized photography by motion picture, press, stereoscopic, and miniature cameras); do metallurgical, ballistics and explosive examinations (guns, bullets, bombs, restoration of serial numbers) provide ultraviolet identifications and surveillances, handle the polygraph (truth detector) examination of suspects; apply modern techniques of microscopy, spectroscopy, serology, and chemistry to minute evidence such as fibres, hairs, blood, poison, textiles, stains, dust, dirt, and debris, provide chemical tests for intoxication and narcotic addition (drunk meter, intoximeter, alcometer, breathalyzer, nalline testing); apply plaster of paris and moulage technique (tool-marks, tiretracks, foot-prints); examine questioned documents for hand writing, type-writing and ink identification); and in general, apply the knowledges and skills of the natural and physical sciences to the solution of crime.

Records and Identification Activities

The administration, organization and management of departmental record processes. Ordinarily, these activities include maintenance of the master's name index, records files for complaint, investigation, arrest, property, identification, location and type of crime, and follow-up reports. Identification activities centre around the processing of fingerprints, photographs, criminal history records, and often include files on aliases, monikers, tattoos and deformities. Field investigation reports are collated and the modus operandi procedures which may utilize highly sophisticated mechanized records are implemented. Information of interest to other agencies is processed, along with information required by state and federal crime reporting units and the data on warrants issued and criminals at large disseminated.

Inspectional Services

They are those which assist, in a very special and sensitive fashion, the administration of the agency and which are primarily dedicated to the elimination of graft, corruption and organized crime.

Intelligence Activities

They are directed to the collection, collation and application of information relating to those members of organized-crime who direct, finance, operate and profit from large-scale gambling, narcotic, prostitution, extortion, liquor law violations and other forms of racketeering. In many agencies, this unit also has the responsibility for the collection, collation and referral of information relating to those individuals (and groups) that are continuously found to be in the centre of labour-management disputes, minority group disturbances and political picketing and whose conception of the common good seems to be manipulated by criteria other than the Constitution and Bill of Rights. The authors would not be surprised to see a substantial

increase in intelligence energy directed to the area of "Upper-world" or "White Collar" Criminals.

SECURITY SERVICE DELIVERY IN ORGANISATIONS AND COMMUNITIES: METHODS AND TECHNIQUES

Service delivery in security industry is the second leg of this paper. Service delivery is defined as a system that provides something that the public needs, organized by the government of any industrial or project authors.

Security service livery can be considered from the following perspectives:

Security Awareness

The security department must create security awareness in his organization or community.

The security executive cannot sell the necessity and importance of the security function to others if his people do not understand it. More often than not, the average Security Department employee has a rather limited view of the security function, seeing it only as it relates to his particular assignment. This "tunnel vision" has a predictable influence on one's attitude, and one's attitude affect one's job performance and relationship with others in and out of the department.

The single most important aspect of retail security is **shrinkage or inventory shortage**. Inventory shrinkage, the difference between the inventory of merchandise on the books and the actual physical presence of goods confirmed by an inventory count, is the one tangible measurement of a security department's effectiveness in protecting assets.

In one retail organization, for example, the shrinkage percentage figure, cause of shrinkage, and goals are discussed on posters, in handouts, and in the Security Department's own publication. Some security personnel do not understand shrinkage and assume that they know how important their respective jobs are. Today security officers must be thoroughly convinced of the need and importance of the department as well as of their respective jobs.

New Employee Inductions

There is certainly no better opportunity to sell security than that afforded at new employee induction sessions, Not only is there a "captive" audience but it is an audience eagerly receptive to information about their new work environment.

Some believe that the presentation of security issues during the induction program should be made by member of line management, even with a prepared script, however, managers tend to deviate from the material, emphasizing those things that they think are important (which may not be) and omitting information that they feel is better left unsaid because it is distasteful, such as the consequences of internal dishonesty.

Consequently, to ensure that hew employees are exposed to the information deemed necessary and appropriate, it must be presented either by a security employee or by way of some form of audiovisual media by security expert.

The personal presentation is by far the better techniques, if and that is important if the security employee is a personable, interesting and effective speaker. The higher the rank of the employee making the presentation the better. Ideally, such presentation should be made by the Security Director. The further down the chain of command this task is delegated, the lower the priority it will be given by the inductees. Then the very objective of the exposure to stress the necessity and importance of security within the organization is defeated.

In a very large organization, spread over a wide geographical area, the Director's personal appearances may necessarily be limited to special events such as the opening of a new facility• Under such circumstances, the use of audiovisuals is a good alternative. Three of the most commonly used audio-visual formats are the slide/tape programme (35 mm color photographs projected on a screen with

accompanying audiotape), a voice message on audiotape, and videotape. All three can be used effectively to orient, educate and sell security for effective service delivery.

Slide/tape and Power Point programs are inexpensive and relatively easy to put together. This particular medium can be used to employees in a graphic and colorful manner what the Security Department does. Such programs can tolerably run 8 to 12 minutes, long enough to develop an interesting message for general personnel education as well as for new employee induction sessions.

Audiotape programs should be shorter, probably not exceeding 4 minutes. For this reason, they are more practical for inductee consumption exclusively.

Video is unquestionably the most effective medium. One of its advantages is that it tends to personalize the guest or speaker so that people can identify with him or her — a feature not available in slide/tape or audiotape programs. Thus, video is the closest to a live personal appearance. These media can, of course, be combined in a presentation Slide/tape or audio programs might conclude with a videotaped interview with the Security Director for added personal impact.

Use of Audiovisuals for Effective Security Service Delivery

The use of audiovisuals in selling security is not limited to new employee orientation presentations. A large commercial organization hotel uses the media described and in addition, short motion pictures produced in-house to dramatize security and safety problems and procedures ranging from the handling of bomb threats to fire prevention. “Capturing” a thief on tape has made the threat of shoplifting truly credible to the people who can do the most to thwart such activities. He has made literally thousands of employee’s consciouses of their role in preventing shoplifting. Such activity has helped to sell the necessity and importance of security.

There are also a wide range of commercially produced 16-mm motion pictures and video cassettes aimed at industrial and business consumers. Even films that do not specially apply to the work scene and Security's role there can help security for example, a film on rape prevention presented by the Security Department for the education of female employees.

Finally, because of the increasing use of multimedia, any kind of security presentation can use a combination of Power Point type programs and videotape and be made available through company local area network as well as wide network systems.

EXECUTIVE ORIENTATION TECHNIQUE FOR SECURITY SERVICE DELIVERY IN ORGANISATION

It is as important, if not more so, to deliver the security message to the management team as it is to the line employees. To ensure this, one organization requires all new incoming middle-management hires to come through the department for a two-hour orientation. The new Controller Unit Manager thus becomes acquainted with department heads and their philosophies. This is certainly not an innovation, yet security is not always included in this type of executive orientation, and it should be.

There is the need to consider the impression made on the new executive. He or she meets the Security Director in the latter's office, where, after light conversation, he or she is given an organizational overview of security. The executive is provided with an organizational chart on which he or she can fill in the names of key supervisors and their phone extensions for future reference. He or she is asked about the security function of his or her previous employer and using that as a comparison, the Security Director emphasizes the differences, pointing out the merits and virtues of the new company's programme over what the new executive is accustomed to. Following that, the executive is introduced to an assistant, who spends time discussing operational practices and problems. Then the executive is introduced to the balance of the

department's staff personnel and is given a tour of security offices.

These new managerial personnel are partially convinced of the importance of security when they arrive, due to the importance attached to orientation schedule and the two hours devoted to security. There is no question in their minds when they leave the offices that the security function is in the mainstream of the business and has a vital role to play.

SECURITY TOURS

Tours of the security facility are a dramatic way to sell security at all levels in the organization. The behind-the-scene look is intriguing to most people, comparable to the fascination capitalized on by the television and movie industry in "cops and robbers" entertainment. To take as class of line supervisors out of their Supervisory Training School and give them a tour of the Security Department usually proves to be a highlight of their entire programme. Seeing the proprietary alarm room, the banks of files and indices referred to in background investigations makes a lasting impression on employees.

BULLETINS

An important aspect of selling is advertising. The power of a strong campaign is well known. Advertising copy has to be directed toward its market, must be interesting and must have some regularity or consistency in terms of exposure. Given these criteria, the Security Newsletter for Management is of utmost importance.

This four-page monthly publication not only keeps company management informed of what contributes to the security organization's goal attainment but it's also used as a source document for meetings and loss prevention discussions.

This type of bulletin is a mental selling and communication tool. People are curious about crime and the unusual contents, especially when viewed with your newspapers and contents of the evening television news. Such events may occur in their neighbourhood or workplace, their interest is intensified. Unless the dissemination of security events compromises security, why not share interesting aspects with other employees? Doing so, it highlights the necessity and importance of the security function.

MEETINGS

Visibility and the opportunity to speak and answer questions about security during company meetings is a powerful way to sell the organization. Because security usually has an impact, to some degree, on every aspect of company life, the Security Department has something of value of contribute to meetings of any department of the company.

The objective is to achieve visibility and a piece of the meeting agenda. As a rule, the person who is calling or conducting the meeting is receptive to enlivening the agenda, and the change of pace and interest that a Security Department representative brings almost guarantees time. There is always an issue to speak to, depending on the composition of the group; for example, at a meeting of the Human Resources Department, Security could talk about recent bond and application falsifications and the importance of Human Resources and Security working together to ensure that only the highest quality applicants are brought into the company.

The Security Director and Security Manager should participate in these meetings but not exclusively. It is important to delegate this function down through all levels of the security organization's structure. This not only helps security supervisors grow but it also establishes an unofficial "speaker bureau" and greater exposure. If there is reluctance to permit supervisors to speak for the development (usually out of fear they will say something that does not meet with management's approval), presentations can then be prepared and practiced in your own training session.

Security's involvement in company meetings can take many directions. In one retail organization, for example, that participation included the following:

1. Regional Store Managers' Meeting, comprising store managers and key staff personnel from one region of the company. During this meeting, the security agent in charge of security within that region could ask for and receive 15 minutes on the agenda, during which he reviewes the policy of scheduling fitting room checkers and related budgetary considerations. Questions and discussion reveal that the topic is timely. The security agent leaves the meeting with a sense of accomplishment. Later, feedback may indicate that the agent made an impressive presentation and that there has been a good dialogue.

2. Human Resources Managers' Meeting. The Security Director asked for 30 minutes to discuss recent conflicts between Personnel and Security over employee disciplinary decisions. The essence of the message is "by virtue of our different responsibilities, we are bound to find ourselves from time to time on collision courses. Why collide? This must be resolved to the satisfaction of both sides, refer the issue up to the next highest level for a direction." If it's a positive and constructive meeting, the Director's time may be extended to 60 minutes.

3. Department Managers' Meeting. The Security Manager can meet with department managers responsible for high loss areas in the business. He discusses contributing causes and suggests ideas on how they could combat such losses, with the meeting attracting a great deal of attendee participation. The loss area under discussion may not due to theft but to "paper errors", "yet Security's presence and interest will be a plus. In the department managers' eyes, the Security Manager may however be seen to be stepping outside his traditional role and assuming a different managerial dimension but he is helping to sell security, as well as coming across as a pleasant and intelligent person who is interested in their problems.

4. Dock Workers' Meeting. A security line supervisor attended a meeting in the warehouse for dock employees. A videotape of a commercially prepared motion picture on internal theft was exhibited. The security supervisor answered questions following the film. This is a' tough situation, to stand up and be willing to take any questions, and the dock workers knew it.

INVOLVEMENT PROGRAMMES

Programmes or activities that bring non-security people into personal contact with the Security Department, with a common goal, tend to cement good relationships.

At one university, for example, students have worked with the Campus Security Department as volunteers. The volunteers are furnished with a security bicycle and two-way radio for shift patrol work. A similar programme exists at another campus, where students voluntarily patrol wooded areas of a large university on their own. They provide this service to the security organization in exchange for the facilities for keeping their vehicles on campus. Not only does the personal involvement have a positive impact on the individual, his or her involvement, if visible to other employees of the company, serves as an example. The logic is simple; if students see other students patrolling areas of the campus, then they realize there must be a need for security and if security is necessary, it is important.

Selling security within the organization sets and maintains a climate of understanding, appreciation and support for the department's objectives. Some of that support comes in the form of budgeted funds.

REFERENCE AND FURTHER READING

Akinade A. (2012) "Private Security Enterprises and Guide Force Management" ISN Publication Series, Lagos

Akinade A. (2012) "Public Policing and Private Security Designs for Maximum Urban Protection" ISN Publication Series, Lagos

Akinade A. (2016) “Public, Private and Community Security System” ISN Publication Series, Lagos

Barnard, C.I. -(1993): The Functions of the Executive. Massachusetts: Harvard University Press.

Bendix, Reinhard and S.M. Lipset (1953): Class, Status and Power Glencoe: The Free Press.

Nis, W.G. (1969): Organisation Development: It Nature, Origin and Prospect. London: Addison-Wesley.

Oyegoke Oyejide (2003): Private Security in Nigeria. Lagos: ISN

Adebayo Akinade (2004): Managerial and Operational Skills for Modern Security Practice. Lagos: ISN

Isaac Ayinde Adalemo (2003): "Security and Safety: Panacea for Enhancement of Democracy and National Development. Lagos: ISN

Ejiogu Aloy M. and G. Harries-Jenkin (1980): Marginal Professionalism: A Study of Teachers Work Values, Durham and Newscastle Review. IX (44), 74-84.

Greewwood, Ernest (1957): Attributes of a Profession. Social work, 2(3), 44-45.

Legatt, T. (1979): "Teaching as a Profession" in IA. Jackson (ed), Professions and Professionalization. London: Cambridge University Press.

Leigh, Paul M. (1979): Ambiguous Professionalism: A Study of Teachers Stat Perception. Educational Review, 34 (1).

Lipset, SOM. and Midred A. Schwartz (1966): The Politics of Professionals in Vollmer, Howard M. and Dod L. Mills (eds) Professionalisation. New Jersey: Prentice Hall.

Newman W.H. (2000): Administrative Action. New Jersey: Prentice Hall.

Onyene, V.E. (2000): Dynamics of Institutional Management:

Towards Strategic Administrative Competence. Lagos: Sam Orient Publishers.

Van Fleet D.D. & Peterson, T.M. (1993): Contemporary Management, New Jersey, Houghton Mifflin Co.

PUBLIC RELATIONS AND COMMUNICATION IN SECURITY AND CRIME PREVENTION

ENHANCING COMMUNITY POLICING THROUGH PUBLIC RELATIONS

Adeola Adesope, fisn

ABSTRACT

More nations are embracing community policing as a tool for addressing the increasing wave of crime and insecurity, mostly at the community and neighbourhood level. Nigeria is not left out of the struggle to curb and fight insecurity, in view of this, it adopted community policing strategy to combat surge in crime. This paper discusses community policing, how it is practiced and why it should be practised and encouraged in Nigeria. It highlights public relations tools that could be applied to community policing to yield maximum benefits and result. It concludes that collaboration and partnership between police and community, which is the main issue in community policing can better be achieved by infusing public relations and community policing.

Keywords: Enhancing, Community Policing, Reputation, Trust. Public relations

INTRODUCTION

Public Relations, whether in commercial or non-commercial organisation seeks to bring the organisation closer to its numerous publics (shareholders and stakeholders). Through deliberate and carefully planned actions, PR professionals project positively, the image of the organisation before its publics. It creates, maintain and sustain good relationship between the organisation and its publics. The benevolence and friendly disposition of organisations toward their publics in the course of doing business is essentially important. Goodwill, an intangible asset helps organisation build good reputation, this can be achieved when organisations consciously identify and relate well with its various publics in order to achieve its set aims and objectives.

Good reputation doesn't just surface, it is sought for, vigorously work for and then achieved. Public Relations, the deliberate professional maintenance of favourable and acceptable public image by organisations serve as a veritable and useful tool to project positive image for organisation, drive goodwill and earn it the good reputation required to survive and achieve success. Organisations make concerted efforts to establish, manage, maintain and sustain good relationship with their publics to achieve good image. Organisations which cherish and value good image have public relations department or engage professional PR organization that monitor the attitude and perception of their publics and then report back to the organization for necessary action.

Public relations maintain control over public opinion of organisations. It involves a wide range of activities carried out by organization to promote, project and protect its image in the psyche of its numerous publics. It is used to manage crises and communication within the organization and between the organization and its publics. It helps organization to choose positive programme of action to address issues and also strive to get rid of actions and inactions which arise due to questionable practices.

Public Relations activity is mutually beneficial to the organization and the public; it aligns the organization's interest with that of the publics. It adopts and embraces two-way communication and not just disseminating information but, listen to the public and actively engage them in conversation. It is practiced at the management level and should be an integral part of the organization decision making organ.

This paper attempts to view community policing through the lenses of public relations. It imbued the various tenets of public relations with community policing in the modern age and explore the possibility of integrating the

ideals of public relations into community policing for enhanced, effective and friendly policing at the community level.

LITERATURE

Community Policing: What it is

Nations world over are shifting away from traditional policing to community policing. The inability or failure of the conventional policing to curb crime and ensure safety of lives and property, especially at the community level, necessitated the search for an alternative policing. Community policing philosophy demands active participation of police within the community. It also requires reorganizing of the police and reorientation of officers to align with the ideologies of community policing. Community policing is collaboration between police and community, with the intention to work out solutions to peculiar security challenges within the community, utilizing resources available to both parties to achieve result.

Trojanowicz and Bucqueroux (1990) cited in Moose (1993; 5): described community policing, as 'a new philosophy of policing based on the concept that police officers and private citizens working together in creative ways can help solve contemporary community problems related to crime, fear of crime, social and physical disorder, and neighborhood decay'. This definition portrays community policing as a concept that requires collaboration between police officers and private members within the community to creatively address security issues and safety. It is a partnership between the conventional police/security agents and individuals/groups which helps to make the community safe and reduce crime. Community policing revolves around the philosophy that the entire community, if worked together, can help take measures to combat and prevent crime. Cossyleon (2019) explained that community policing is implemented differently and in different context, its aim is to address the changing security needs of communities.

Community policing is established on a doctrine which acknowledges the association and shared duty/authority of the police and community in making community safe and in peace. It encourages partnership that identifies community security challenges, decides resources, and put in creative plan of action outlined to produce and sustain healthy, safe and crime free-community. Community policing synchronizes efforts of police, individuals, and stakeholders to produce an all-inclusive approach to the community's problems of crime, disorder and other security challenges. It reflects the values of: community involvement; problem solving; officer role in decision making; accountability of the police; and deployment of security personnel at a level closer to the community. According to Mulugeta and Mekuriaw (2017: 1) 'Community policing is a paradigm shift established at the bedrock of community partnership in creating safe and secure environment for all'.

How is Community Policing Practiced?

There is no universally accepted standard for community policing. Community policing basically, is the collaboration between the police and the community that identifies and provides solution to security problems in the community. In this collaboration, police seize to be the sole guardians of law and order but, all members of the community. The police and other stakeholders in the community become active partners in the struggle to ensure the safety and quality of the community. Community policing strategies vary depending on the needs and responses of the communities involved; however, certain basic principles and considerations are common to all community policing efforts (Bureau of Justice Assistance, 1994).

It is the duty of police to give talks to the community on the purpose, intention and the benefits of community policing. Community policing is a universally accepted idea which is devised for modern policing; being an ideal measure to curtail crime, especially at the community level, police should utilize it optimally. Community policing requires the collaboration and support of the members of the community to succeed. It is the duty of police to make concerted effort to encourage and convince the community to partner with it in order to ensure safety and security of lives

and propriety in the community. Though, the community has a lot to benefit from community policing in the long run, but the police is supposed to be at the forefront of the campaign for community policing because, it is the organization that is constitutionally responsible for enforcing law and order.

Police needs to encourage vigilantes and neighborhood watch groups in the community to assist it in the enormous task of ensuring safety of lives and property. These groups, which perhaps understand the terrain and the people more than the police officers assigned to the community, will adequately compliment the efforts of the police officers thereby making the job easier. These groups will serve as link between the police and the community which will make relationship between the two cordials.

Community policing requires the use of foot or bicycle patrol. Roads in some communities are bad and not motorable which makes vehicle patrol almost impossible. Also, the 'Aberdeen patrol' whereby police patrol vehicle is used by security personnel to patrol an area periodically is not ideal for community policing, immediately the patrol team leaves the area anything can happen. The ideal is to have more police officers permanently stationed.

Police need to identify and partner with stakeholders such as business organizations, community leaders, traditional leaders, trade groups, media etc. The media plays significant roles in the society. The establishment of community-based media will go a long way at helping achieve the goals of community policing. One of the reasons why communities own radio stations is for security purpose. The media will assist the community to hear and be heard, share current ideas and educate the people on trending issues on crime and criminality among other things.

Security is everybody's business but police is at the vanguard of law enforcement and crime prevention therefore, police is expected to educate the people at the community level on crime prevention methods. Police should advice and give talks regularly to vigilantes and neighborhood watch; this will encourage them and also serve as corporate social responsibility on the part of the police.

It is necessary to create special team of police officers to work, monitor and follow up on community policing. These teams should be specially trained and dedicated to community policing and provide progress reports regularly. The officers involved must be accountable to the community they serve.

There must be clear cut communication between the police and the community as regards the objectives and strategies to be adopted. Communication must be a two-way and not otherwise. This will give the community a sense of belonging and it will be willing to be more committed to the course.
The idea of centralized police will isolate it from the communities and the people it is serving. For a practicable and purpose driven, efficient and effective community policing, decentralization of the police authority is very necessary. This will create opportunity for self-reliant and improved initiative which will allow sound discretion among the rank and file. What works or applicable to community 'A' might not be in community 'B' due to difference in culture, tradition, language, religion, terrain, beliefs etc.

Why Community Policing

Increasing insecurity all over the country create doubt about the ability of the country's security apparatus to handle the numerous security challenges being experienced. People live in endless fear and succor is not even near, they are at the receiving ends, owing to the loss of their property and loved ones. In an attempt to manage insecurity and reduce crime, people at the community level organized vigilantes and neighborhood watch. Another effort to ensure security of lives and property at the community level is the creation of 'police community relationship committee'. This committee comprises selected members of the community which relates with police on security matters. Definitely, it is not business as usual, just as the people are eagerly searching for lasting peace in their community

the police are also willing to partner with the people to achieve their goal, which is to have a peaceful and livable community.

The following reasons may have necessitated the need for community policing:

1. The realization that government and community must jointly accept responsibility for ensuring peace and safe community.
2. Policing strategies that worked in the past are no longer effective.
3. Dwindling economic situation and challenges are adversely affecting government revenue. The decreasing government revenue is reducing allocation to the police which in turn affects its operations. The police are underfunded which makes it unable to perform up to expectation.
4. The police have not been able to singlehandedly manage crime successfully at the community level.
5. Increasing wave of crime and criminality at the rural level and neighborhood.
6. Shortage of police officers and concentration of the available few in cities and as orderlies to political office holders, politicians and their allies.
7. There are democratic tendencies in community policing. It gives the people opportunity to have a say and be actively involved in matters that affect them. It is the security of the people by the people and for the people.

Importance of Community Policing

Community policing creates strong ties between the police and the community. Without this the police may lose favour with the people and it may also not have access to information it needs from the community that could help it tackle crime.

Community policing allows established relationship between the police and various interests in the community. If well managed, this in turn will create trust among the partners' such that helpful ideas, information and assists will be coming from community members.

Community policing provides opportunity for both the police and the community to work together to sort out serious security problems that exist in the communities where internal dispute exists or, in a situation where relationship with the police have been seriously strained. Community members will begin to perceive the police as part and parcel of the community when they believe the police are genuinely interested in and committed to community perspectives and issues.

Community bodies and groups are usually the first means of addressing social disorder and crime at the community level. In view of this, it is necessary that the police partner and work intimately with those groups within the community to spot issues of concerns and come up with effective remedies. This is the crux of community policing.

Community policing accords the police better image. People who live in communities where community policing is practiced are more likely to make favourable comments about the police. The partnership will bring the community people closer to the police and vice versa, thereby creating a robust and friendly environment which views the police as partners in progress.

Community policing emphasis is on crime prevention; it promotes public safety and enhances the quality of life in the community where it is practiced. Since all stakeholders in the community are all actively responsible to ensuring safety of lives and property, there is the tendency that the community will enjoy peace and the quality of lives of people in the community will be better off.

Why Community Policing Should be Introduced and Practice in Nigeria

Governments all over the world have realized that they can no longer monopolize the business of security (Kasali and Odetola, 2016). The job of securing requires the active participation of every individual and institutions. Safeguarding the welfare of the country and its wellbeing is the responsibility of all and sundry. This suggests that everybody

must work and pull resources together to ensure the safety of lives and property.

It is widely believed that the conventional policing method has failed and can no longer, solely guarantee effective crime control especially at the community level. In addition, policing and the police are far from the community. There is the need to draw policing nearer and closer to the people at the community level. Kasali and Odetola (2016: 102) states that,

The relationship between police and civil community in Nigeria has been considered by many as unfriendly such that the men and officers of the police institution are often perceived by the public as those without any sense of responsibility, integrity and commitment to duties. From the evolution and functions of Nigeria Police, the public police are often considered as stooges of the state whose loyalties wholly lie with the political elites and their cronies.

The police and the people had become so separated from one another, so much that in some communities an attitude of us versus them exists between the police and the people. The emergence and adoption of community policing will eradicate this mentality, bring the people and police together as business partners and foster good relationship. The adoption of community policing into Nigeria's security arrangement will erase the bad opinion which Nigerians have about the Nigeria Police. It will unite and create strong ties between the people and police.

Nigeria is a complex nation of many nations with diverse culture and tradition. A centralized police authority is not ideal for a federation of 36 states and a federal capital territory comprising 774 local governments. The country is faced with numerous security challenges ranging from kidnapping, terrorism, human trafficking, drug peddling, armed robbery, rape/defilement, banditry among others. The security architecture of the country finds it very difficult, if not impossible to manage these menaces. In view of this, there is public opinion that top echelon of the security agencies be replaced. The replacement would amount to nothing if the approach and method of securing the country is not rejigged. Security personnel and security approach are likened to computer hardware and software. The two complement one another, no matter how well or bad one is it will have effect on the other. Therefore, the two are expected to be up to the challenge because they cannot work without one another. The necessary security software needed at this crucial time in the life of Nigeria is 'community policing'. It will bring police and other security agencies closer to the grassroots and change the entire face of policing from what it used to be. There is no better time than now to completely entrench the doctrine of community policing into the country's security arrangement.

Community policing was initiated in Nigeria in April 2004, by former President Olusegun Obasanjo in collaboration with the Nigeria Police Force, under the supervision of former Inspector General of police, Mr. Tafa Balogun. Since then, much has not been heard of community policing until the increasing wave of insecurity which led to the agitation for state police and the eventually creation of 'The Amotekun Corps' in the western region of Nigeria. The outfit has a coloration of community policing and it is meant to serve the people and complement the police at the community level.

Combining community policing and the traditional crime fighting strategies will effectively address security challenges facing the country. Community policing does not take away the constitutional role of the police, the authority to police and preserve law and order is still vested in the police. However, the police should consider tapping into the resources that is available at the community level; this will definitely relieve police of some of its burdens. Finally, community policing is universally recognized and practiced therefore, Nigeria cannot be left out. Not only has it been recognized globally, it has recorded success in many countries because it is regarded as the alternative security management strategy.

Strategies to do Enhanced Community Policing through Public Relations

Flynn (2004) cited in Kasali and Odetola (2016: 100) states that, 'the success of the outcome of the partnership between the police and community largely lies on the amount of trust that exists in their relations'. 'Without trust between police and citizens, effective policing remains elusive'. Partnership is built on trust and can only work and survive on trust. People will not like to go into partnership with people they don't trust. Trust is depending and believing in others that they will not hurt or pose any form of risk to their partners. Trust is the bedrock of relationship. The United Nations Peace Operations Manual (2018) asserts that, trust between police and community will increase when community works together with police to make the community safe. This will also make the community rely on the police and entertain less fear. The trust will encourage the community to report crime activities within the community to police and other relevant information that will be useful to the police in crime fighting.

The *Bureau of Justice Assistance (1994: 13) posits that, 'to develop community partnership, police must develop positive relationships with the community'.* In some communities, there still remains a general mistrust of police and unwillingness among residents to share information about neighborhood crimes with the police. This information is essential to police enforcement activities as well as prevention efforts (Diamond and Weiss, 2005).

There are two core complementary components in community policing namely; community partnership and finding solution to identified problems. For community partnership to work, police must establish positive relationship with the community, involve the community in the quest for enhanced crime control and prevention also, the resources of both the police and the community must be harnessed to deal with the urgent concerns of the community.

The issue of partnership is germane in community policing. It is the bond and life blood of community policing without which its success is not guaranteed. People are likely not going to partner with people who lack good reputation therefore; the Nigeria Police must work hard to earn good reputation so it will earn the respect of the people to the extent that people will be willing to partner with it to make community policing a success story in Nigeria. Gregory (2010: 37) posits that,

A good reputation is not something that is earned overnight. It has to be carefully and considerately cultivated. It is something that is earned over a period of time as understanding and support develop for an organization. The management of reputation has to be meticulously undertaken with integrity and honesty. It is something that is very fragile and can be lost quickly if words and actions are found to be out of sympathy with reality.

Reputation is earned by what one does and not by what one says. It may be difficult to measure but, its value and importance to either an organization or an individual is definitely indisputable. Broom (2009) explains that public relations is about reputation – the result of what you do, what you say, and what others say about you. The question now is what are people saying about the Nigeria Police? Does the Nigeria Police have a good reputation such that people will be willing to partner with it in the "Nigeria community policing project". Broom (2009: 25) states further that,

Public relations are the discipline which looks after reputation, with the aim of earning understanding and support and influencing opinion and behavior. It is the planned and sustained effort to establish and maintain goodwill and mutual understanding between an organization and *its publics.*

Public relations are described as the ideal panacea for earning good reputation. One of the core components of community policing is partnership, between the police and the community. It is widely believed that people will be willing to partner only with individual or organization with good reputation

therefore, to achieve an effective and workable community policing, the police must work assiduously to earn and retain good reputation; this can be done by adopting public relations philosophy and activities.

Another function of public relations that can be applied to advance the course of community policing is community relations. Community relations as a function of public relations positively put forth the organization's messages and image within the community (Seitel: 2011). This approach is aimed at fostering good relationship between the police and the community. Having established a relationship with the community, community relations will help the police to nurture the existing relationship, this will strengthen the ties and will in turn earn the police good reputation which will keep the flag flying and good for community policing.

Organizations should be seen as responsible citizen of their community, the police inclusive. Community relations activities of the police should focus on building a positive and respectable image for itself in the community. Community relations programmes such as corporate social responsibility, counseling and educational talks on how to prevent crime will help to build good reputation for the police and benefit the community. Door to door visit to the community by assigned police officers can be beneficial and aid community policing effort. Such visits can be used to introduce new officers to the members of the community, get information about crime happening in the community and to offer good and needed information to members of the community on security education.

As part of its community relations activity, the police can organize town meetings regularly. This will assist the police in maintaining contact between it and the community which is essential for the anticipated success of community policing which it spearhead. This meeting will create an avenue for communication between the police and the community such that ideas, information, opinion and the likes will be shared. It will also serve as a ground for evaluation of what has been done and how to improve on it. The police can also create relationship with groups within the community; members of the community belong to at least one of such groups. This will bring the police more closer to individuals, groups and the community as a whole.

Conclusion

Increasing insecurity and the failure of the existing security arrangement to curb crime has necessitated the need for review of the security architecture of Nigeria. The current security disposition is obsolete and need to be reviewed or replaced. Community policing is the new strategy being adopted all over the world to curtail crime, it is recognized as the possible antidote to insecurity, but has not been implemented in Nigeria as done in other climes. Community policing was introduced into the Nigeria security system in 2004. Since then, government has continued to promote it as an alternative security strategy to reduce crime.

Partnership and collaboration to jointly solve security problem are the two cardinal factors in community policing. It requires the police and the community to work together for a common goal of ensuring safety of lives and property. For community policing to succeed, there must be a cordial relationship between the police and the people, the people must be willing and ready to partner with police otherwise, community policing will not be a success story in the country. Partnership and collaboration can be managed by public relations, hence the need to apply it to community policing.

The hostile attitude of the Nigeria Police toward the people is an impediment to community policing in the country. The image of the police is bad and need to be worked upon for acceptability by the people. Public relations will help the police to focus on strategies that promote positive public relations that will allow enhanced community policing. Public relations are an effective strategy for the police to earn public trust. Public relations should be implanted into the

operations and activities of community policing.

References

Broom, G. M. (2009). *Cutlip and Center's effective public relations* (10th ed.). London: Pearson

Bureau of Justice (1994). Understanding community policing: A framework for action. *US Department of Justice NCJ 148457.* Retrieved September 24, 2020 From https://www.ncjrs.gov/pdffiles/commp.pdf Cossyleon, J. (2019).

Community policing. *The Wiley Blackwell Encyclopedia of Urban and Regional Studies.*

DOI:10.1002/9781118568446.eurs0058. Retrieved September 18, 2020 Fromfile:///C:/Users/PROGRA~1/AppData/ Local/Temp/Cossyleon2019.Communitypo licing.pdf

Diamond, D. and Weiss, D. M. (2005). *Community policing: Looking to tomorrow*. Washington D. C.: US Department of Justice. Retrieved September 18, 2020 From

https://www.masc.sc/SiteCollectionDocuments/Public%20Safety/community%20poli cing.pdf.

Gregory, A. (2010). *Planning and managing public relations campaigns* (2nd ed.). London: Kogan Page

Kasali, M. A. and Odetola, R. G. (2016), Alternative to policing in Nigeria: Analyzing the need to redefine community policing in tackling the nation's security challenges. *African Journal of Criminology andJustice Studies: AJCJS, Vol.9, Issue 1*. Retrieved September 18, 2020 From https://www.umes.edu/uploadedFiles/_WE BSITES/AJCJS/Content/VOL9.%20KASALI%20%20FINAL.pdf.

Moose, C. (1993). *The theory and practice of community policing: An evaluation of the Iris Court demonstration project.* (Ph. D. Thesis, Portland State University, USA) Retrieved September 18, 2020 From https://core.ac.uk/download/pdf/37773277 .pdf.

Mulugeta, E. and Mekuriaw, D. (2017), Community policing: Practice, roles, challenges and prospects in crime prevention in East Gojjam administrative zone. *Social Crimonol* 5: 160. doi: 10.4172/2375-4435.1000160. Retrieved September 24, 2020 From https://www.longdom.org/open-access/community-policing-practice-roles-challenges-and-prospects-in-crimeprevention-in-east-gojjam-administrative-zone-2375-4435-1000160.pdf.

Seitel, F. P. (2011). *The practice of public relations* (11th ed.). New Jersey: Pearson

United Nations Peace Operations Manual (2018). Community-oriented policing in United Nations Peace Operations. Retrieved September 18, 2020 From https://police.un.org/sites/default/files/manual-community-oriented-poliicing.pdf.

INSTITUTE NEWS AND INFORMATION BULLETIN

GOODWILL MESSAGE

Mr. Olawale Fatolu, dfisn
Distinguished Fellow, Institute of Security, Nigeria

Distinguished Ladies and Gentlemen
I would like to congratulate the Institute of Security for organizing this conference. The Institute of Security has always maintained that the issue of security service and law enforcement in Nigeria is not simply a criminal justice reform issue but that of national security. Security reform requires a holistic approach.

Indeed, security system in Nigeria requires a total overhaul in order to attain effectiveness, efficiency and Professionalism. Making progress within security system needs great coordinated attention in order for the exercise not to be in futility.

In essence, what is being suggested is that there must be a master-plan or blue print for the entire security, system including private security architectures. This conference is a step in the right direction. It is believed that the problems of security will be discussed frankly with tested solutions. We recognize that though no one can claim to be a repository of this solution to the multifarious problems of this country but there is too much at stake in our nation today hence this conference cannot be merely an exercise in the theoretical and technical overview of the state of security in Nigeria. We are confident, knowing the calibers of participants and resource persons, that this conference has gathered, they will no doubt unravel the mystery puzzle in due course.

We urge all the security agencies to partner with the Institute of Security of Nigeria and other professional bodies in the presentation to the nation of a comprehensive blueprint for a sound National security system policy. This exercise will guarantee Nigeria sound and amiable security, law and order system in which all Nigerians, investors, local and foreign will be and feel secured.
It is suggested that the government must engage in the massive appropriation of funds to the building of modem and indeed functional security equipment and facilities. Modem technological equipment and facilities will guarantee quicker and more institutional realization of the objectives of security, law and order to achieve efficiency and enhanced productivity. There is the need for proper re-integration and cooperation among the security organizations.

VALUES OF PROFESSIONALISM AND NIGERIA SOCIETY

Values are fundamental principles, standards, the individual and societal source of rights and wrongs. The moral foundations and ethical principles that guide human and societal conduct. These are the bedrock and foundation of best practices and professionalism in security sector.

These virtues and guidelines are reflected in laws, norms and policies that guide professions, a nation and its people. To a great extent, the larger section of humanity recognizes certain fundamental values which drives the society.

Values are reflected in human character and conduct. Character in leadership is very vital and it is the foundation of every best practice and professionalism.

Character is very essential of human person. They are the mental and moral qualities distinctive to an individual, the personality, nature, disposition, temperament, mentality, psyche, psychology, constitution. make-up of an individual. This is what makes an individual a leader, what he is, how he will make policy, execute policy and react to the society he leads.

There is the need to introduce and implement security technology such as weapons screening programmes, entity control systems, video cameras and scanning. Metal detectors either handheld or portal types, efficiently detect the presence of firearms, knives and explosives.

Attention should be directed to solutions to terrorist attacks, kidnapping, banditry, transportation accidents, natural disasters and political and social violence, plane crashes, bomb blasts because-they bring unseen burdens to public safety agencies.

Conclusion

In conclusion, I greatly appreciate the activities of the Institute of Security and hereby convey my best wishes. I congratulate all awardees, the distinguished fellows, professional fellows, professional members and associate members at this conference now being conferred on them. Thank you.

GOODWILL MESSAGE

Dr. Cynthia Gregg, dfisn
Distinguished Fellow, Institute of Security, Nigeria

I welcome you wholeheartedly to the 16th Annual Conference of our Institute. The theme of this year's conference is "**Exploring Best Practices and Enhanced Professionalism in Security and Police Architecture in Nigeria**"

The theme is indeed a most fitting one, having regard to the current security challenges confronting our nation, The security system has always had an important and critical role to play in tackling these challenges.

Let me take advantage of this opportunity to share with you my views on some of the issues that must be addressed if the security system is to discharge its obligations to ensure effective and efficient security operations and provide adequate anti-crime and security coverage in Nigeria.

The stakeholders in security services include public security agencies and private organized security organizations. All of them are active participants in the security architecture process. Thus, the success or failure of the security and law enforcement system is bound to impact on society's economic, social, political, stability and well-being of the nation. The success of the security system is inextricably linked to the survival of the entire Nigerian state.

Insecurity and the threat to the maintenance of law and order have assumed a frightening and alarming dimension in present day Nigeria. The scepter of terrorism looms large and threatens the very existence of the nation. The activities of the terrorists, kidnapers and similar militant groups easily underscore the rising stakes in respect of their destructive campaigns. The destabilizing impact of unrestrained and routine destruction of lives and property in the Nigerian state is worrisome and should be a matter of concern for all of us.

I am referring to the situation in which innocent civilians and, in some cases, law enforcement agencies are targeted by bombing or the explosion of various incendiary devices. This has created terror in the people and a resultant lack of confidence in the system. Nigerians are concerned and look upon the government and law enforcement agencies to live up to their constitutional responsibility of securing their lives and property.

It is noted that the whole society has been enveloped by a nauseating craze for the acquisition of money and material wealth at the expense of decency. brotherly love, moderation and the fear of God. It is advisable that the government should be determined to tackle the problem by taking pro-active steps which will enable government to be ahead of the situation. Efforts should be taken to contain the excesses of these terrorists by appropriate evaluation of their objectives and tactics with a view to countering them effectively. The option of dialogue could also be explored if situational and strategic analyses show, that this is a viable approach to the solution of the problem(s) which fuel(s) the insurgency and that dialogue is needed to restore peace in troubled spots.

This year's conference theme takes into consideration the foregoing security nightmares that the nation is currently experiencing. The conference seeks to unravel the measures to be taken in order to make our security system responsive to the needs and aspirations of Nigerians through best practices and professionalism. It is our hope that the resource persons will, in the process of their presentations and discussions, endeavor to provide feasible solutions to the identified problems. It is noted that the security agencies operate in a disjointed, uncoordinated and

disharmonious manner. It should he emphasized that the security of the nation is far too important to be sacrificed on the altar of political expediency and personal or group interest.

The security and law enforcement system are in need of reform similar to the situation in the United States of America following the disaster of 2001. We do not need to wait until we experience a disaster of such monumental proportions before taking necessary action to reform our security system. What is needed is the identification of the major inadequacies, problems and obstacles that are responsible for the current unsatisfactory performance of the security system. Nigerians deserve effective and accountable security forces to counter violent extremism as well as a coordinated campaign to ensure the protection of economic activities and sustained development. It is not enough to pretend to tackle the problem by merely throwing money at it as we have done via the 2012 national budget, we have to think out of the box to unravel the causes of the ineffectiveness of our security system. The problem of insecurity is not limited to any inadequacy in the quality of the personnel who currently man the various security and law enforcement outfits. The people currently heading our security agencies are all competent men who are capable of the tasks they are constitutionally assigned to do.

The problems, it seems to me are manifold and include the following:
(a) Our national culture and attitude towards the nation-state;
(b) The current domestic security structure;
(c) The current national security paradigm;
(d) The self-immolating governing system that is currently in place;
(e) The inadequacies in the constitution that currently guides us;
(f) Our weak and fragmenting institutions,

There is no doubt that as we focus our attention on the improvement of the security institutions, there is need to also address those factors that constitute security challenges of our country. Indeed, our current security challenges must be resolved holistically. This must include the examination of issues such as the complementary roles of citizens and communities in the fight against terrorism; the neutralization of extreme ideologies and intolerance and the development of appropriate responses to economic and social insecurities.

Apart from discussing the issues of the security institutions and the reforms that are essential to our development and secured existence, it is vital to examine that very important factor — we the people of Nigeria.

What exactly do we want? Do we truly desire a system of security that works or are we merely paying lip-service to this subject-matter? What is our attitude towards the dispensation of security and law enforcement?

The people of Nigeria, to a large extent, determine the institutions which serve as instruments of governance in the country indeed our Institutions mirror us. For a security practitioner to practice successfully in the 21st century he must constantly update his skills and venture into new frontiers. This is because security personnel interact in the course of discharging of their professional duties with all manners of persons and with diverse array of subject matter. They therefore need to be constantly updated on a wide variety of security issues and topics. Even in his own area of specialization, the security practitioner must be up-to-date with all developments in his chosen area.

From what has been observed above, it should be obvious that we are not getting the desired output from the security system. It is better to approach this issue by asking a number of

rhetorical questions some of which include and border on the efficacy of our security system. Do we have a security system that safely secures the lives and property of Nigerians? Are the security agencies capable of providing services to the whole of Nigeria having regard to the present manner and circumstances of its existence? Why are economic crimes, violent crimes and serious white-collar crimes on the increase?

Distinguished ladies and gentlemen, there is clearly palpable frustration, even anger, in the inner-most thoughts of Nigerians that progress has not occurred fast enough inspite of the fact that providence has favoured our beloved country with abundant resources. The paradigm of tethered horses unable to benefit from the abundant food made available to them because they were pulling in different directions should provide a lesson for us in Nigeria. As long as we ponder to ethnic or regional interests to the detriment of national interests, for so long shall we continue to suffer deprivation in the midst of plenty. In this regard, I venture to suggest that an active civil society is absolutely an essential instrument to combat corruption, serve as the conscience of the nation and hold elected officials accountable. Benefiting from the resources of the nation must not be dependent on where one has come from — a mere accident of birth over which none of us has any control.

Conclusion

The need to review and overhaul the present security system cannot be over-emphasized. It requires that we all be disciplined and focused. We must change our approach to national issues if we are to succeed as a nation. Our security system must be thoroughly refurbished and strengthened. It is not about wanting to rub shoulders with technologically advanced nations or seeking to be a permanent member of the Security Council of the United Nations just to boost our ego as a nation. It is about making realistic changes which will enable us put our house in order and earn the respect of other nations.

VOTE OF THANKS

Col Moses Aderemi Oketola (Retd), fisn
Secretary, Institute of Security, Nigeria

Your Excellencies, Distinguished Guests, Special Guests of Honour, Ladies and Gentlemen, I stand before you with a deep sense of honour, privilege and humility to express, on behalf of the President of the Institute of Security Nigeria to express our profound appreciation to all of you here today, for sparing time to attend the opening ceremony of the conference and Investiture ceremony. May the good Lord reward you all for your labour of love, which has been manifested in terms of your presence here today.

The speakers have laid due emphasis on the need and importance of the roles played by the police and security professionals in any democracy and crucial aspects. Your speeches and messages have laid the foundations and will serve as an inspiration for our ensuing deliberations.

I want to use this occasion to specially thank the Vice-Chancellor of the University of Lagos, Professor Folasade Ogunsola dfisn, for her support and encouragement to the Institute. May your tenure be characterized by peace and progress with remarkable achievements in the University of Lagos.

We appreciate the Chairman Professor Omololu Soyombo dfisn and Patron, Prince (General) Dr. Olu Bajowa dfisn for being present at the occasion. The distinguished guests of honours, the Key Note Speaker AIG (Dr.) Bala Hassan dfisn and presenters of goodwill messages and the various contributors are highly appreciated.

The words of wisdom and the various thought-provoking contributions in the opening ceremony are quite apt and have set the right tone for solving the problem of political and education challenges. There is the need for innovation, provision of best practices and professionalism in the police and security architecture. There is the urgent need for national strategy to improve the quality service delivery in and strategic intervention and strengthening law enforcement for crime prevention and security of lives and property of the citizens.

Distinguished ladies and gentlemen, this conference could not have come at a better time considering the security challenges in the country and need for national integration, as well as the need for capacity building and improvement of training skills in addressing these challenges. The best practices and skills in the security system, integrity and ethical system discussed are appreciated.

National security and efficient security system are determinants of development in every area of the polit. We need to note that democracy cannot thrive in an atmosphere of insecurity, corruption and violence.

We appreciate your support for the institute towards actualizing its objectives. We highly appreciate your sound commitment to the promotion of the culture of quality security and safety in Nigeria.

May you continue to excel in your professional and social endeavours as you assist in spreading the spirit of quality security and safety for the emergence of a better nation which we shall all be proud of.

Thank you.

PROFILE OF THE 3rd PRESIDENT

Distinguished Prof. James Dele Olowokudejo
FLS, FLEAD, FCFIP, FIAF, dfisn

Distinguished Professor Dele Olowokudejo holds a B.Sc. Special Honours Degree in Botany from the University of Lagos and a Ph.D. degree from the University of Reading, England, in Plant Taxonomy and Biosystematics. His experience spans over 45 years of University Teaching, Research, Curriculum Development, Consultancy and Community Services. He has published over 100 scholarly research articles in peer-reviewed national and international high impact journals, and presented more than 200 papers at conferences, symposia and workshops on Biodiversity, Medicinal Plants, Natural Resources Management, Environmental Assessment and Sustainable Development. He has been a visiting Scholar and Researcher to many reputable Universities and Research Institutes all over the world and has supervised and graduated eighteen (18) Ph.D. including NUC Best Ph.D. Thesis Student Award in Biological Sciences in 2011. He is a diligent teacher, an active researcher and a prolific writer.

Professor Olowokudejo is a Recipient of several Fellowship Awards including those of the Linnean Society of London, Rockefeller Foundation Leadership for Environment and Development, Royal Society of Great Britain, The British Council, Association of Commonwealth Universities and the International Institute of Certified Forensic Investigation Professional Inc; USA. He was a recipient of many Academic Scholarships such as Federal Government of Nigeria, National Undergraduate Merit Award, German Scholarship and Western State of Nigeria Scholarship. He won the J. F. Kennedy Memorial Essay Competition at the zonal level in the Western Region.

He was a member of the University of Lagos Senate and Governing Council; Chairman, Management Board of Centre for Information and Technology Systems; Academic Programmes Committee of the Postgraduate School. He is also a member of the University Senate, Staff Welfare Advisory Board; Administrative and Technical Staff Committee; Finance and General Purposes Committee and Council Committee on Accreditation of Academic Programmes, among others. At various times Professor Olowokudejo served as Dean of Student Affairs Division, Head of Department of Botany and Microbiology; Chairman of Students Disciplinary Board; Chairman of, Governing Board of Distance Learning Institute; Board of Trustees of University of Lagos International School; Senate Committee on Quality Assurance; Academic Programmes & Curriculum Review; Students Scholarships, Loans and Bursaries Board. Professor Olowokudejo also served as a member of the Planning and Implementation Committee of Elizade University, Ilara-Mokin, Ondo State and Trinity University, Laloko, Ogun State; Panel of Assessors of Correspondence Colleges in Nigeria and the National Universities Commission Accreditation Panel. He is an External Examiner and Academic Assessor to several Universities and other Tertiary Institutions. He was an African Representative to the UNESCO- ICSU World Conference on Science in Budapest, Hungary (June-July,1999).

Professor Olowokudejo was conferred with the Distinguished Professor Award at the 2019 Convocation Events of the University of Lagos "in recognition of his sterling contributions toward promoting and advancing knowledge in the society through quality research, teaching and mentoring young scholars". Other honours received included the University of Lagos Long Distinguished Service Award; Distinguished Researcher in Science and The Rockefeller Foundation Award.

He is happily married to Dr. Folake Feyisayo and they are blessed with children.

PROFILE OF AIG (Dr.) Hassan Bala, fwc, psc+ npm, dfisn
Keynote Speaker

Hassan joined the Police Force in 1982 as Cadet Assistant Superintendent and worked in several places in Nigeria including Police Commissioner in Edo, Aba, Rivers and Borno States. He was a commissioner in charge of Police Legal Departments as well as Police Force (MOPOL). He was AIG and Commandant of the prestigious Police Staff College, Jos and also AIG in Zone 9 Sokoto and Zone 2 Lagos. He attended various universities in Nigeria including Ahmadu Bello University, University of Ilorin, University of Ibadan, University of Lagos, University of Science and Technology, Port Harcourt, Nigeria Law School Lagos, National Defence College, Abuja.

He bagged a doctorate degree in Policing, Security and Community Safety from London Metropolitan University

Dr Hassan Bala is a distinguished teacher who fostered innovative teaching methods and techniques in security, policing, criminal justice and crime prevention managements. He is a foremost police and law professional who garnered recognition in the practice. Hassan has a longstanding commitment to interdisciplinary teaching and research. He is a promoter of effective teaching and learning environment which reinforced his commitment to the excellent teaching and works which expand his reach and impact globally. With his rich experience in police, security and legal practices he provides enviable and excellent leadership in the frontiers.

Hassan's professional and scholarly development offerings for the area of specialization is unique. He is passionate about best practices and scholarly in legal and security disciplines.

He is married with children.