THE APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) IN CRIME PREVENTION IN THE FACE OF GLOBAL SECURITY CHALLENGES.

By

Amaobi Uwaleke, B.sc, M.sc, M.sc.IT, Ph.D, Maitp, Mais, Fnii, Miee, Fcai.

DEPARTMENT OF INFORMATION TECHNOLOGY, FEDERAL UNIVERSITY OF TECHNOLOGY OWERRI.

INTRODUCTION

The modest approach to this topic is for us to define the keywords in this topic probably because of the nature of the topic and the nature of the audience. Information is an essential need of man after food. The next thing man need to survive is information, all human races, the old, the young, man and woman need information to survive. The battle of greatness among nation is fought in the laboratories and in the field of information gathering, processing, and dissemination.

Information can be defined as assemblage of processed data when consumed by the user it increases the mental capacity, increases the knowledge base, and wipes away the state of uncertainty. Any information that did increase the mental capacity and the knowledge base of the consumer is not information. Information can be regarded to be as old as man. Our great, ancestors used information to locate where they hunted successfully; they also used it for security and defense. In the present day Nigeria, information is an indispensable tools for governance and other aspect of our daily life.

Communication can be described as the imparting or exchange of information by speaking writing, or using some other medium such as televisions, radios, newspapers are effective medium of communication. Communication can also be

in form of transmission or better still imparting, conveying, reporting, presenting, passing on, handling on or relay.

Technically speaking communication can be described as the transfer of data from the transmitter to the receiver. Therefore communication must have a medium of transmission such medium can be through manual medium like talking, clapping of hands, body movement, eye signals or by other medium such as digital transmission, analogue transmission. The major difference between digital and analogue transmission, rest on the shape of the frequency of transmission. While digital transmission is discrete, analogue transmission is continuous.

The world communication was derived from the Latin world 'communicare' meaning to share it is actually the activity of conveying information through the exchange of thought, message, or information, as by speech, visuals, signals, writing, or behavior.

One definition of communication that cut across so many definitions is any act by which one person gives to or receives from person information about that person's needs, desire, perceptions knowledge, or effective state. Communication may be intentional or unintentional, may involve conventional or unconventional signals, may take linguistic or none-linguistic form, and may occur through spoken or other mode.

Communication requires a sender, a message and a recipient, although the receiver doesn't have to be present or aware of the sender's intent to communicate at the time of communication thus communication can occur across vast area or distances in time and space.

Communication requires that the communicating parties share an area of commonality and the communicating process is complete once the receiver understands the sender's message.

Technology can be defined as the application of scientific knowledge for practical purpose especially in industries, services and advances in computer applications. Technology originates from Greek word 'teckne' which means art, skill, and cunning of hands. It is actually the making, modification, usage, and knowledge of

tools, machine, technique, craft, systems and method of organization in other to solve problems and improve pre-existing solutions to a problem and achieve a goal and handle an applied input/output relation and or perform a specific function. Technology can equally means collection of tools including machinery, modifications, arrangement, and procedures. Technologies significantly affect human as well as other animals' ability to control and adapt to their natural environment. The term can either be applied generally to specific areas: examples include construction technology, Medical Technology, Policing Technology and Information Technology, Dancing Technology etc. There is Technology in every thing, therefore Technology is a way of doing things.

Human species use of technology can be traced to the era where natural resources were converted to simple tools. The pre-historical discovery of their ability to control fire, increased the available sources of food and the invention of wheel help human in travelling in and control their environment. The recent technological development including printing press, the telephone, and the internet and Intranet have lessened the physical barrier to communication and allowed humans to interact free in a global scale. However technology cannot be said to have improved the life of man only it has also made the life of man miserable, this is evidenced in the development of weapon of mass destructions, nuclear weapons, sophisticated war heads, chemical weapons etc.

Technology has affected society and its surroundings in a number of ways in many societies, technology has helped to develop and advanced their economies, and has allowed the rise of leisure class but at the same time produced some unwanted by-product such as pollution and deplete natural resources to the detriment of the environment. However the introduction of technology has actually turned the globe into a village where all human endeavors can be said to be wheeled by technology.

Crime can be said to be an action or omission which constitute an offence and is punishable by law such action like shoplifting, stealing raping etc. offence is an unlawful act , illegal act, breach/infraction of the law, misdemeanor, misdeed, wrong, felony, violation, transgression, fault, injury and more. The term crime in

modern times does not have any ending definition generally accepted but one out standing definition is that a crime also called an offence or a criminal offence is an act harmful not only to some individual but also to the community or the state such act are forbidden and punishable by law.

When one commits a crime, the state has the power to severely restrict the person's liberty for committing that crime, therefore in modern societies, a criminal procedure must be adhered to during the investigation and trials only if found guilty that the offender may be sentenced to punishment.

Having discussed the major components of this topic, it is now important for us to look how Information technology can help in crime prevention and management. The world we are living today is burdened with insecurity, as result of poverty, religious in-tolerance, environmental degradations, as well as political instability.

In modern policing the application of information and communication technology has actually increased the efficiency of police men and other security Agencies.

Criminologist such as Gottfredson, Mckenzie, ECK, Farriton, Sherman and others have been at the forefront of analyzing what works to prevent crime some prestigious commissions and research bodies, such as the World Health Organization, United Nations, United States National Research Councils, The UK Audit Commission etc, have analyzed their and other research on what lowers rate of interpersonal crime.

They agreed that government must go beyond law enforcement and criminal justice to tackle the risk factors that cause crime because it is more cost effective and leads to greater social benefits than the standard way of responding to crimes. Interestingly, multiple opinion polls also confirm public support for investment in prevention through the deployment of information and communication technology. Waller uses materials in his 'less law more order' to propose specific measure to reduce crime as well as crime bills using information technology.

The World Health Organization guide (2004) complements the world report on violence and health (2002) and the 2003 World Assembly Resolution 56-24 for governments to implement nine recommendations.

1. Create, implement and monitor a national action plan for violent prevention.
2. Enhance capacity for collecting data on violence through ICT Applications
3. Define priorities for, and support research on the causes, consequences, cost, and prevention of violence
4. Promote primary prevention responses through the creation of data bases.
5. Strengthen responses for victim of violence.
6. Integrate violence prevention into social and educational policies and thereby promote gender and social equality.
7. Increase collaboration and exchange of information on violence and prevention through provision of ICT infrastructure like Internet, Intranet and Extranets for security Agencies.
8. Promote and monitor adherence to international treaties, law and mechanisms to protect human rights.
9. Seek practical, internationally agreed response to the global drugs and global arms trade.

The authoritative commissions agree on the Role of Municipalities, because they are best able to organize the strategies to tackle the risk factors that cause crime. The European Forum for Urban Safety and the Unity States Conference of Mayors have stressed that municipalities must target the programs to meet the needs of youth at risk and women who are vulnerable to violence.

To succeed, they need to establish a coalition of key agencies such as schools, job creation, social services, housing and law enforcement around a diagnosis.

Several factors must come together for a crime to occur.

1. An individual or group must have the **desire** or motivation to participate in a banned or prohibited behavior.

2. At least some of the participants must have the **skills** and tools needed to commit the crime; and,

3. An **opportunity** must be acted upon.

Primary prevention address individual and family level factors correlated with later criminal participation. Individual level factors such be attachment to school and involvement in pro-social activities decrease the probability of criminal involvement.

Family level factors such as consistent parenting skills similarly reduce individual level risk. Risk factors are additive in nature. The greater the number of risk factors presents the greater the risk of criminal involvement. In addition there are initiatives which seek to alter rates of crime at the community or aggregate level.

For example, Larry Sherman from the University of Maryland in Policing Domestic Violence (1993) demonstrated that changing the policy of police response to domestic violence calls altered the probability of subsequent violence. Policing hot spots, areas of known criminal activity, decreases the number of criminal events reported to the police in those areas. Other initiatives include community policing efforts to capture known criminals. Organizations such as America's Most Wanted and Crime Stoppers these help catch the criminals.

Secondary prevention uses techniques focusing on at risk situations such as youth who are dropping out of school or getting involved in gangs. It targets social programs and law enforcement at neighborhoods where crime rates are high. The use of secondary crime prevention in cities such as Birmingham and Bogota have achieved large reductions crime and violence. Programs that are focused on youth at risk have been shown to significantly reduce crime.

Tertiary prevention is used after a crime has occurred in order to prevent successive incidents. Such measures can be seen in the implementation of new security policies following acts of terrorism such the September, 11, 2001 attacks.

Situational crime prevention uses techniques focusing on reducing on opportunity to commit a crime. Some of techniques include increasing the difficulty of crime, increasing the risk of crime, and reducing the rewards of crime.

Situational Crime Prevention

Introduction and Description

Situational Crime Prevention (SCP) is a relatively new concept that employs a preventative approach by focusing on methods to reduce the opportunities for crime. SCP focuses on the criminal setting and is different from most criminology as it begins with an examination of the circumstances that allow particular types of crime. By gaining an understanding of these circumstances, mechanisms are then introduced to change the relevant environments with the aim of reducing the opportunities for particular crimes. Thus, SCP focuses on crime prevention rather than the punishment or detection of criminals and its intention is to make criminal activities less appealing to offenders.

SCP focuses on opportunity-reducing processes that:

- Are aimed at particular forms of crime;
- Entail the management, creation or manipulation of the immediate environment in as organized and permanent a manner as possible; and
- Result in crime being more difficult and risky or less rewarding and justifiable.

The theory behind SCP concentrates on the creation of safety mechanisms that assist in protecting people by making criminals feel they may be unable to commit crimes or would be in a situation where they may be caught or detected, which will result in them being unwilling to commit crimes where such mechanisms are in place. The logic behind this is based on the concept of theory behind SCP concentrates on the creation of safety mechanisms that assist in protecting people by making criminals feel they may be unable to commit crimes or would be in a situation where they may be caught or detected, which will result in them

being unwilling to commit crimes where such mechanisms are in place. The logic behind this is based on the concept of rational choice – that every criminal will assess the situation of a potential crime, weigh up how much they may gain, balance it against how much they may lose and the probability of failing, and then act according.

One example of SCP in practice is automated traffic enforcement. Automated Traffic Enforcement Systems (ATES) use automated cameras on the raods to catch drivers who are speeding and those who run red lights. Such systems enjoy use all over the world. These systems have been installed and are advertised as an attempt to keep illegal driving incidences down. As a potential criminal, someone who is about to speed or run a red light knows that their risk of getting caught is nearly 100% with these systems. This completely disincentivizes the person from speeding or running red lights in areas in which they know ATES are set up. Though not conclusive, evidence shows that these type of systems work. In a Philadelphia study, some of the city's most dangerous intersections had a reduction of 96% in red light violations after the installation and advertisement of an ATES system.

Applying SCP to Information Systems

It has been suggested that the theory behind situational crime prevention may also be useful in improving information systems (IS) security by decresing the rewards criminals may expect from a crime. SCP theory aims to affect the motivation of criminals by means of environmental and situational changes and is based on three elements:

- Increasing the perceived difficulty of crime;
- Increasing the risk; and
- Reducing the rewards.

Information Systems professionals and others who wish to fight computer crime could use the same techniques and consequently reduce the frequency of computer crime that targets the information assets of businesses and

organizations. Designing out crime from the environment is a crucial element of SCP and the most efficient way of using computers to fight crime is to predict criminal behavior, which as a result, makes it difficult for such behavior to be performed. SCP also has an advantage over other Information Systems (IS) measures because it does not focus on crime from the criminal's viewpoint. Many businesses/organizations are heavily dependent on information and communications technology (ICT) and information is a hugely valuable asset, which means Information Systems has become increasingly important. While storing information in computers enables easy access and sharing by users, computer crime is a considerable threat to such information, whether committed by an external Hacker (computer security) acker or by an 'insider' (a trusted member of a business or organization). After viruses, illicit access to and theft of, information form the highest percentage of all financial losses associated with computer crime and security incidents. Businesses need to protect themselves against such illegal or unethical activities, which may be committed via electronic or other methods and Information Systems security technologies are vital in order to protect against amendment, unauthorized disclosure and/or misuse of information. Computer intrusion fraud is a huge business with hackers being able to find passwords, read and alter files and read email, but such crime could almost be eliminated if hackers could be prevented from accessing a computer system or identified quickly enough.

Despite many years of computer security research, huge amounts of money being spent on secure operations and an increase in training requirements, there are frequent reports of computer penetrations and data thefts at some of the most heavily protected computer systems in the numerous illegal activities, including email surveillance, credit card fraud and software piracy. As the popularity and growth of the Internet continues to increase, many web applications and services are being set up, which are widely used by businesses for their business transactions.

In the case of computer crime, even cautions companies or businesses that aim to create effective and comprehensive security measures may unintentionally produce an environment, which helps provide opportunities because they are

using inappropriate controls. Consequently, if the precautions are not providing an adequate level of security, the Information Systems will be at risk.

Situational crime Prevention and Fraud

In computer systems that have been developed to design out crime from the environment, one of the tactics used is risk assessment, where business transactions, clients and situations are monitored for any features that indicate a risk of criminal activity. Credit card fraud has been one of the most complex crimes worldwide in recent times and despite numerous prevention initiatives, it is clear that more needs to be done if the problem is to be solved. Fraud management comprises a whole range of activities, including early warning systems, signs and patterns of different types of fraud, profiles of users and their activities, security of computers and avoiding customer dissatisfaction. There are a number of issues that make the development of fraud management systems an extremely difficult and challenging task, including the huge volume of data involved; the requirement for fast and accurate fraud detection without inconveniencing business operations; the ongoing development of new fraud to evade existing techniques; and the risk of false alarms.

General, fraud detection techniques fall into two categories: statistical techniques and artificial intelligence (AI) techniques.

Important statistical data analysis techniques to detect fraud include:

- Grouping and classification to determine patterns and associations among sets of data.
- Matching algorithms to identify irregularities in the transactions of users compared to previous profiles.
- Data pre-processing techniques for validation, correction of errors and estimating incorrect or missing data.

Important AI techniques for fraud management are:

- Data mining – to categorize and group data and automatically identify associations and rules that may be indicative of remarkable patterns, including those connected to fraud.
- Pattern recognition to identify groups or patterns of behaviour

CONCLUSSION.

The importance of ICT application in the Nigerian Police is highly desirable I would like to see the rebranding of the police force to be ICT compliance. The establishment of intergrated crime database for Nigerian Police Force so that the police can effectively participate in the global crime fightintg efforts.

There is a need for the force to modify its policy for ICT acquisition so that the force can enjoy all the advantages provided by this new technology.

I would like to see in the police force where the Inspector General of police will sit in the comfort of his office and hold conferences with his commissioners of police and police top ranks, using Virtual Realty Technology (VRT). This Technology short cuts the need for travel out of their stations.

I would like to see a police force that deploys UAVs for surveillance and area mapping for the purposes of fighting crimes.

Finally full stream ICT applications in the activities of Nigerian police will be a welcome development.