THE LEGAL FRAMEWORK AND INSTITUTIONAL ARRANGEMENT ON THE USE OF ICT FOR DETECTION AND PREVENTION OF CRIMINALITY AND INSECURITY AT ALL LEVELS IN AFRICA

BEING A PAPER PRESENTED BY:
DR. DAUDA CHIKA
PSIN – Abuja (Nigeria)

AT THE HIGH LEVEL INTERNATIONAL CONFERENCE ON ICT AS A MODERN SOLUTION TO SECURITY THREATS AND EARLY DETECTION AND PREVENTION OF CRIMES

TANGIER (MOROCCO)
23-25 JUNE 2014
“The Police of today needs the technology of 3 years from now in other to prevent criminals who have tomorrow’s technology yesterday”

Introduction:

1.0 The proliferation of modern and complex information communication technology (ICT) including the borderless connectivity of the World Wide Web (www) have significantly altered the way nation states deals with their security, political, economic and social issues. While the western and developed countries have taken advantage of developments in the ICT to improve on their legal and institutional arrangements in crime detection and prevention, Africa have grossly lagged behind and have not leveraged on these 21st century tool in addressing its myriad of security and other challenges. (1)
Advancement in technology has come with a lot of challenges and new methodology of crime: criminal groups and clandestine organizations been well financed, and with a great deal of knowledge in the use and application of ICT, have perfected Computer related misdemeanor such as cyber stalking, computer hacking, copyright infringements, money laundering, identify theft, Bank theft, and child pornography with alarming speed and across jurisdiction. There is a paradigm shift from the Traditional,/National crimes to a more sophisticated and highly rewarding criminal enterprise of cyber related offences of extortion, advanced fee fraud (or 419 in Nigeria) yahoo. yahoo, cyber terrorism and internet Banking fraud. (2)
The global character of the ICT has enabled criminals to take advantage of weak state institutions and flawed regulatory systems in Africa to commit illegal activity with impunity, making it essential for law enforcement in Africa to as a matter of necessity adopt their domestic crime fighting strategy to the cyberspace and use modern ICT in crime detection and prevention. (3)
2. Insecurity and criminality is a complex and dynamic phenomenon sometimes associated with the socio-economic, cultural and political history of most Africa States. At the national level, most countries in Africa have witnessed: (4)

- **Electoral violence and fraud resulting in bad governance, lack of political accountability and impunity.**
- **Armed violence by insurgent groups, ethnic militia men and terrorist groups.**
- **Youth unemployment, and porous state boarders**
- **Weak institutional and regulatory arrangements**
➢ Proliferation of small arms and light weapons resulting in protracted and recurring violent conflicts

➢ Intense conflict between groups engendered by political, religious and ethnic intolerance largely engineered by the elites and executed by exploiting the ignorance, vulnerabilities and poverty of the majority of the citizens.
Understandably, this climate of insecurity and criminality is now a feature of our modern world, for two main reasons, first, because of the lowering of economic and political barriers and secondly because of the advancement in communications and commerce. Insecurity and criminality generally, is the darker side of our contemporary world as science and ICT have provided the convenience and anonymity with which crimes may be committed. (5)
A. INFORMATION AND COMMUNICATION TECHNOLOGY (ICT):

ICT refers to the technology, services and applications used in the process of communications. The World Bank defined ICT as “consisting of hardware, software, network and medium for the collection, storage, processing, transmission and presentation of information (voice, data, text, images) as well as related services.

ICT can be split into ICI and IT i.e. (that is) information and communication infrastructure (ICI) which refers to the physical information Technology or telecommunication systems and IT i.e networks (celular, broadcast, cable satellite, postal) and the services that utilize them, that is the internet voice, mail, radio and television. (6)
B. DETECTION AND PREVENTION:

Approaches to crime detection and prevention are reflected in nation states policies and regulations. Emphasis is not only on how crime can be reduced but also on how to reinforce and maintain social cohesion and improve on the quality of life of citizens without infringing on their fundamental rights.

The following are the features of crime detection and prevention:

i. Crime prevention through social development
ii. Community prevention mechanism (community policing, vigilante etc)
iii. Situational crime prevention
iv. Witness protection programme/victim compensation (7)
C. CRIME/CRIMINALITY

A crime is a reprehensible human conduct which is sanctioned and punished by law.

A crime is (simply) a wrong which affects the security or wellbeing of the public generally so that the public has an interest in its suppression: criminality is a moral wrong that amount to a conducts which is inimical to the general moral sense of the people and community. (8)
D. INSECURITY:

Insecurity is the absence of security; Security is paramount to the state, community and individual and the sole responsibility of state. Security is the aggregation of the interest of a group, political entity, institution or individuals within a geographical location. It implies a stable, relatively predictable environment in which individuals or groups may pursue their legitimate objectives and means of livelihood without inhibition, disruption, harm, danger and fear of injury. (9)
3. ADVANTAGES OF ICT IN CRIME DETECTION AND PREVENTION:

3.1 Modern Technology (ICT) provides a new method of crime detection and prevention. Deployment of ICT in crime prevention requires political, economic, technological and managerial catch-up to fill the gaps created by years of misgovernance. Deliberate and conscious efforts must be made by African Leader and Policy Makers to:-
➢ Design a wholistic national ICT policing strategies.
➢ Appropriate resources and budget to ICT
➢ Training and retraining the regular and combat officers on the use of ICT in crime prevention and detection
➢ Insist on ICT knowledge as a prerequisite for recruitment.
➢ Extension of the effective use of ICT tool in crime prevention to the judiciary, the court systems and the justice ministry/department.
3.2 WEAKNESSES

Crime and security experts have identified the following weaknesses in the use of ICT (Information Communication Technology) in crime detection and prevention.

- Lack of ICT knowledge among judicial/law officers, security officers and police.
- Inadequate funding of security and police establishments.
- Weak judicial, legislative and prison system
- General apathy to prompt reporting of crimes for fear of victimization and criminalization
- Cultural and attitudinal in-deference to ICT knowledge
- Cost of ICT
- Availability and maintenance of ICT (electricity, location, service disruption and drop calls)
- Bureaucratic and command structure of law enforcement and police
4. TYPOLOGY OF ICT TOOLS IN CRIME DETECTION AND PREVENTION

This paper takes a cursory look at the utilization of the following ICT tools in the detection and prevention of crime and insecurity generally:

i. Finger Print Analysis

Finger printing is the science of using the patterns of ridges on fingertips for identification purposes. Finger print has been an important part of evidence since its invention over 100 years ago. (10)
Finger print obtained from the scene of a crime are photographed, scanned and compared with the data of previous offenders (print) for match. The service makes use of powerful pattern matching computers, to make the task of finding a match quicker. – Most police formation’s and law enforcement agencies have perfected this age long art for early crime detection mechanism but proper usage have been hampered by cost and availability.
ii. DNA Profiling

DNA is the genetic code held within every cell in the human anatomy. Every individual has a unique DNA profile specific to his genetic formula. As an ICT tool to defect crime, DNA sample are obtained at crime scene for analysis. The DNA profile is build up by the computer marking and storing the compared DNA swap from other samples earlier obtained (II).

The system uses samples obtained from mouth swabs, blood sample, semen, bone, tissue and other organs or human anatomy.
iii. Police National Computer

The Police have also evolved a wide range of networked computer systems for gathering data and criminal intelligence informations.

The police computer information system have been shared by the national and Interpol across the African subcontinent. The system is usually connected to other databases such as car registration database, and details of individuals who have committed crime in the past. The system sometimes run on the automated fingerprint identification system (FPIS). It is suggested that this system be extended to Embassies and consulate offices to check the activities of terrorists and International criminal syndicates.
iv. Cellebrite device:

Forensic analyses use information obtained from mobile phones of suspects to establish their complicity in a crime. Cellebrite device is a forensic extraction device commonly used by law enforcement agencies, military and corporate security agencies in over sixty (60) countries of the world. The device has an inbuilt mechanism that protects the data extracted which is automatically transferred to a computer.
This device was used recently by the EFCC in Nigeria in a case now pending in the Federal High Court sitting in Abuja. In the said case, the forensic analyst with the EFCC, Maktar Bello, on May 2014 told the Federal High Court how Dodo Chilla Bulus, an Assistant Superintendent of police (ASP) connived with vandals to break pipelines and siphon crude oil – from the NNPC underground pipelines.
The cellebrite device enabled the analyst to establish effective communication and nexus between the accused person and the suspect, by using a computer running on Microsoft operating system a to extraction and harvest information from the suspect’s mobile devices (12).
v. Automatic number plate recognition:

This system is used in the United State and other advanced nation, the Vehicle owner’s personal information is almost always associated and retrievable from the database of stored registration numbers. The system is always fitted in police patrol vehicles in the United State and Britain. This system is recommended for police formations in Africa.
vi. Video and CCTV

Video and CCTV camera are an essential component and tool in ICT usage to combat and prevent crime. Most African countries have experimented this method of crime detection but with little success. In Nigeria for example, the government had over the past 8 years invested over 37 billion naira on CCTV across major cities such as Abuja, Lagos and Port-Harcourt, with little or no success.

The system have falling into disuse because the system was originally designed to fail, not properly monitored and fraught with corrupt practices in the award and execution of the contract.
vii. Social media

The police and security agencies have over time taken advantage of social network such as twitter and facebook to keep abreast with the prevalence of crime in the society. Terrorist groups have also resorted to the use of social media to create an atmosphere of extreme fear, recruit and solicit financial contributions and Boast of their exploits. The on-going Boko Haram imbroglio in Nigeria and the at-shibab claims of responsibility for terrorist acts are clear examples of the illegal use of social medial by criminal groups, in recent times.
viii. Police patrol vehicle

The police use this ICT tool in their every daily routine crime detection and prevention mechanism. Typically, the police patrol vehicle is equipped with:

* Video camera mounted on the windscreen to record incidents as they unfold
* Video camera linked to the automatic number plate recognition system
* Radio equipment
* Speed detector gear
5.0 **CHALLENGES:**

The challenges Associated with the use of ICT in the detection and prevention of crime may include:-

i. Criminal and unauthorized use of ICT to harvest personal information of law enforcement officers/employees and corporate entities for blackmail or to intrude on operational plans (13).
ii. Use of ICT to infiltrate, or coarse the behaviour of law enforcement officers, corrupt official or employees in private sectors e.g. Banks and large corporations.

iii. Exploit the hardship and vulnerabilities of citizens, police, employees etc

iv. Create fear, panic, or uncertainty in the society, community or nation state.

v. Create anxiety and radicalization
6.0 GOALS

Understanding the use and application of ICT in the detection and prevention of crime is a key element in the success of the strategy to combat crime at all levels.

The methodology in the use of ICT to detect and prevent crime would include:-

a) Reducing the opportunities for the commission of the crime (the police law and enforcement must be pro-active).
b) Identify the motives, methods, hotspots, goals and pattern of crime and location (employ GPS or unmanned drones, aircrafts and or artificial intelligences)

c) Establish/create a criminal data Bank and profile of crimes and criminals (types, methods, frequency, finger print impression and photo ID of interrogated criminals)

d) Improve the intrusive capabilities of the police, SSS, DSS including promulgating or enacting legislation empowering covert surveillance military and string operation.
e) Use of wide range of video, CCTV cameras in public places streets, parks, market places, train stations, offices, Bus terminals, airport, churches, mosque, parties and political gathering

f) Use Global Positioning System (GPS) tracking system to determine the positions and locations of vehicle, person fugitive, harmful substances, damaged oil pipe line and vandalism.
G) Financing and activation of (police and other security agencies)
i. Automated finger printing information system (AFIS)
ii. Integrated Ballistic information system (IBIS)
iii. Traffic Ticketing System (TTIS)
iv. Crime Information Management System (CIMS)
v. Mobile Phone and Social Media
vi. Forensic Testing and DNA Capacity
REFERENCES

1. International Report 2010


6. Search security

7. Chamblis W. (1975) towards a political economy of crime theory and society
8. John B. Sauders (Br. ______ 1988)


10. www.teach.ict.com/gcse

11. www.teachriet.com/gcse

12. https://efccnigeria.org