

# The Use of ICT Tools in Tackling Insecurity and Terrorism Problem in Nigeria

A.I. Oludare<sup>1\*</sup> O.E. Omolara<sup>2</sup> A.M. Umar<sup>3</sup> D.V. Kemi<sup>4</sup>

1.Nigerian Defence Academy, Department of Physics, Kaduna

2.Ahmadu Bello University, Department of Mathematics, Zaria, Nigeria

3.Energy Commission of Nigeria (ECN)

4.Nasarawa State University, Department of Mathematics, Keffi, Nigeria

Corresponding author:email: aioludare@gmail.com

## ABSTRACT

The paper seek ICT tools solution to crime and insurgence attack in Nigeria by providing a broad view of the Public Security Communications System (PSCS), Public Safety Networks (PSNs) and National Security Information Centre (NSIC) and some ways that ICT-based technologies can assist security agencies in been more efficient and effective in their operations for national development. In addition, some efficient and effective techniques to tackle insurgency was presented.

**Keywords:** PSCS, PSNs, NSIC, Insecurity, Crime, Insurgency, Boko-Haram, Nigeria

## 1. Introduction

The use of Information and Communication Technology (ICT) in the provision of solution to human, social and industrial challenges has proven success in many nations and Nigeria should not be an exception. According to the World Bank, ICT's —consists of the hardware, software, networks, and media for the collection, storage, processing, transmission and presentation of information (voice, data, text, images), as well as related services [1]. The World Bank further states that ICT can be split into ICI and IT. Information and Communication Infrastructure (ICI), refers to —physical telecommunications systems and networks (cellar, broadcast, cable, satellite, postal) and the services that utilize them Internet, voice, mail, radio, and television).

Reports over the years show alarming increase in levels of crime and Boko Haram terrorist attack especially in the North Eastern Nigeria [2]. Unfortunately, this situation is spreading across the other Africa countries, with countries such as Cameroun, Chad and Niger has now recording disquieting increases in crime levels and attack of Boko-Haram, as Boko Haram Attacks Killed Over 1,000 Civilians in February this year 2015 [3].

There have been various call for the use of ICT tools to tackle security problem in Nigeria [4]. Computer Warehouse Group Plc (CWG) and Huawei have jointly advised the federal government to deploy Internet Protocol surveillance as a technological solution to insecurity challenges facing the country [5]. The greatest contemporary challenge to national security is the insurgency orchestrated by the Islamic sect called Boko Haram. Not until 2009, insurgency and its concomitant effects (both emotional and physical) were alien to Nigeria. Nigeria, most especially, the North Eastern regions of the country; and of recent in Kano, Kaduna in the North Western States, Plateau State and Abuja in the North Central were there has been ceaseless terrorist attacks. The problem led to the Federal Government declaration of state of emergency in the three affected states in the North Eastern Nigeria in 2012. The Government has recently further seek the assistance of foreign nations that are technologically developed such as USA, France, Britain, Israel and others to tackle the menace of Boko-Haram insurgency.

The persistence of insecurity has been claiming precious lives of citizenry and government efforts to tackle the problem through various menial methods and approaches such as the use of police, military, vigilante and local hunters seem not to be yielding success. But deploying technology, through the use of ICT devices such as computer, internet, mobile phone, close circuit television (CCTV), surveillance cameras, social network analysis, biometry surveillance, data mining, satellite imagery, and IP devices, the satellite would definitely produce the desired results." Another strong argument is that besides its speed, technology-driven surveillance and intelligence gathering cost less in terms of men and logistics [6].

Reports shows that the United States and some countries in Europe, Asia, Middle East and even in Africa are taking proactive steps at checkmating threats to their national security by latching onto revolutions in ICT[7]. Nigerians watched in amazement how America deployed its security system to track down the April 13, 2013 Boston Marathon bombers. Similarly, in less than five minutes the images of the two men who hacked down a brave soldier on London Street on May 22, 2013, appeared on television screen around the world. There were no guess works in those scenarios, which make many Nigerians get disturbed by the many cases of unresolved high profile crimes in the country.

The role of ICT in tackling crime in modern times cannot be overemphasised, going by the modern tactics deployed by the western world in tackling crimes. The solution to the nation's insecurity challenges lies

in science and technology such as the use satellite technology to monitor the activities of the insurgents [8]. But of course the cause of the crisis must be identified.

**Definition:** Crisis is the situation of a complex system (family, people, economy, society) when the system functions poorly, an immediate decision is necessary, but the causes of the crisis are not known at times.

## 2. A Crisis System:

- (a) a complex system – a complex system enter crises while, a simple system do not enter crises. We can speak about a crisis of moral values, an economical or political crisis, but not a motor crisis.
- (b) poor function system. The system still functions, but does not break down.
- (c) an immediate decision is necessary to stop the further disintegration of the system.
- (d) the causes are so many, or unknown, that it is impossible to take a rational, informed decision to reverse the situation.

## 3. Crisis Planning

According to Fink, successful crisis planning removes much of the threat and uncertainty in potential future crises, and allows for more control should a crisis appear in (Paraskevas 2006). Despite Fink approach to crisis planning being fairly old, dating back almost 26years, it mirrors the approach of current management. Fink (1986, p. 20-28), stated that a crisis can consist of as many as four different and distinct stages:

- (i) Prodromal crisis stage
- (ii) Acute crisis stage
- (iii) Chronic crisis stage, and
- (iv) Crisis resolution stage. (ibid.)

Fink's statement goes to show that any crises can be described as being in any of the four stages. It is important to identify early warning signals for the crisis, even though it might be hard to recognize them especially crises in a prodromal state. A crisis may be apparent to a community or a state. Yet no action is taken to prevent it. Once the community has passed the initial stage, the crisis will start causing harm depending on how well prepared and effective the community is. The third stage is referred to as the clean-up stage. The community try to retrieve from the crisis and learn from the mistakes it made and the success of it crisis response. In the final stage the community goes back to normality, and resumes with its business as usual. (Paraskevas, 2006)[9].

## 4. Crisis Characteristics

Crisis has several defining characteristics. *Seeger, Sellnow, and Ulmer* say that crises have four defining characteristics that are "specific, unexpected, and non-routine events or series of events that [create] high levels of uncertainty and threat or perceived threat to an organization's high priority goals." Thus the first three characteristics are that the event is;

1. unexpected (i.e., a surprise)
2. creates uncertainty
3. is seen as a threat to important goals

Venette argues that "crisis is a process of transformation where the old system can no longer be maintained." Therefore the fourth defining quality is the need for change. If change is not needed, the event could more accurately be described as a failure.

Apart from natural crises that are inherently unpredictable (volcanic eruptions, landslide, tsunami etc.) most of the crises that we face are created by man. Hence the requirements of their being 'unexpected' depend upon man failing to note the onset of crisis conditions. Some of our inability to recognise crises before they become dangerous is due to denial and other psychological responses that provide succour and protection for our emotions.

## 5. Theory on Crisis Situations

Whether in community, organizational, family, or individual contexts, research on crisis situations is guided by several relevant theories. Some of the most frequently cited of these theories include:

- Apologia theory (Ware & Linkugel, 1973)
- Chaos theory (Seeger, 2002)
- Crisis theory (Halpern, 1973)
- Diffusion theory (Rogers, 2003)
- Excellence theory (Grunig & Hunt, 1984)
- Family resilience theory (Walsh, 1996)
- Image restoration theory (Benoit, 1997)

### 6. A Crisis Situation in Science

A crisis situation can be explained in science, take for example in a classical mechanics system of a harmonic oscillator, when displaced from its equilibrium position, experiences a restoring force,  $F$ , proportional to the displacement,  $x$ :

$$\vec{F} = -k\vec{x} \dots\dots\dots \text{equation (1)}$$

where  $k$  is a positive constant.

If  $F$  is the only force acting on the system, the system is called a **simple harmonic oscillator**, and it undergoes simple harmonic motion. Any motion that repeats itself at regular intervals is called harmonic motion. The figure 1 showed a simple harmonic motion where curve a, 0 and b swing or oscillate between  $-x$  and  $x$  continuously this may be compared to a crisis situation.

A simple harmonic oscillator is an oscillator that is neither driven nor damped. It consists of a mass  $m$ , which experiences a single force,  $F$ , which pulls the mass in the direction of the point  $x = 0$  and depends only on the mass's position  $x$  and a constant  $k$ . Balance of forces (Newton's second law) for the system is

$$F = ma = m \frac{d^2x}{dt^2} = -kx. \dots\dots\dots \text{equation (2)}$$

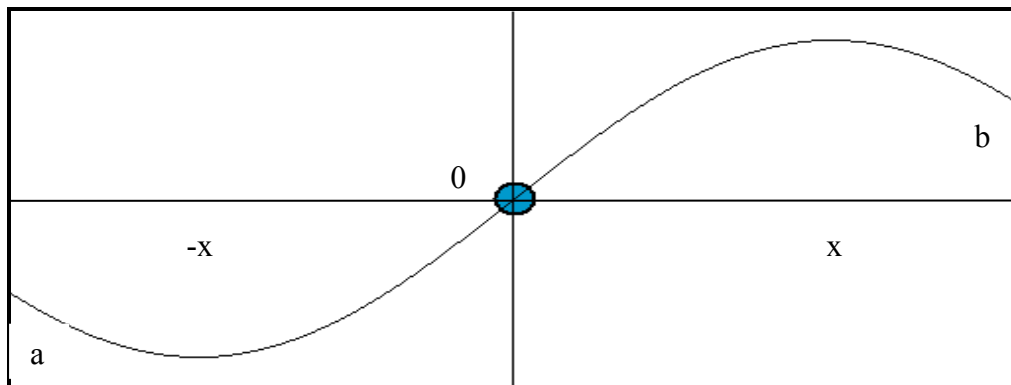


Figure 1: A simple harmonic motion

Solving this differential equation, we find that the motion is described by the function

$$x(t) = A \cos(\omega t + \phi), \dots\dots\dots \text{equation (3)}$$

where

$$\omega = \sqrt{\frac{k}{m}} = \frac{2\pi}{T}.$$

The insurgency attack is periodic, this can be applicable to the motion that is periodic, repeating itself in a sinusoidal fashion with constant amplitude,  $A$ . In addition to its amplitude, the motion of a simple harmonic oscillator is characterized by its period ( $T$ ), the time for a single oscillation or its frequency  $f = 1/T$ , the number of cycles per unit time. The position at a given time  $t$  also depends on the phase,  $\phi$ , which determines the starting point on the sine wave. The period and frequency are determined by the size of the mass  $m$  and the force constant  $k$ , while the amplitude and phase are determined by the starting position and velocity. The velocity and acceleration of a simple harmonic oscillator oscillate with the same frequency as the position but with shifted phases. The velocity is maximum for zero displacement, while the acceleration is in the opposite direction as the displacement. The potential energy stored in a simple harmonic oscillator at position  $x$  is

$$U = \frac{1}{2}kx^2. \dots\dots\dots \text{equation (4)}$$

Again, a crisis system, situation or society can be explained in terms of a damped harmonic oscillator (controlled crisis system). That is in real oscillators, friction, or damping, slows the motion of the system. Due to frictional force (insurgency attack), the velocity decreases (stable society becomes unstable, thus crisis multiplied)

in proportion to the acting frictional force (insurgency attack). While simple harmonic motion oscillates with only the restoring force(applied solution), acting on the system, damped harmonic motion experiences friction. The figure 2 presents the amplitude of a damped harmonic oscillator having an undamped frequency  $\omega_0 = 1$  rad/sec, a damping coefficient of 0.1, an initial position of zero, and a derivative at zero of one sec<sup>-1</sup>. The damping causes a reduction in oscillating frequency to  $\omega_d = 0.995$  rad/sec. The dashed blue lines in the plot indicate the maximum amplitude of the oscillation.

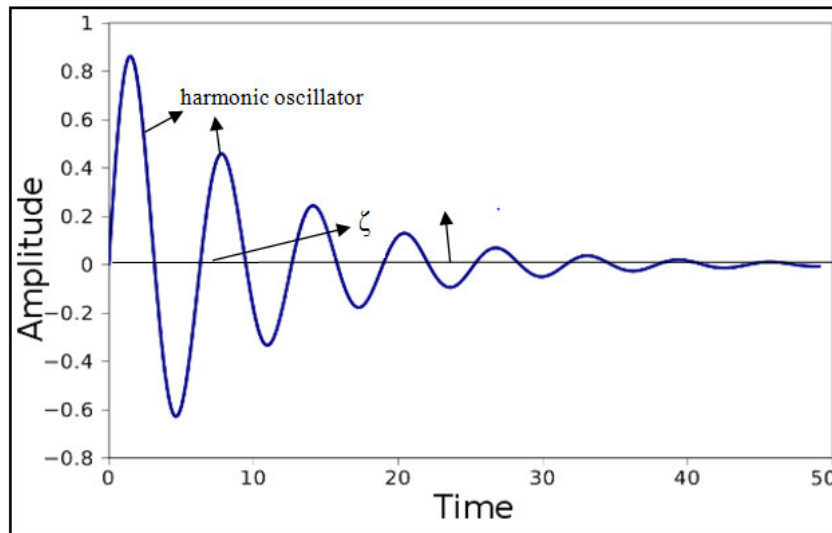


Figure 2: Amplitude of a damped harmonic oscillator.

In many vibrating systems the frictional force  $F_f$  can be modeled as being proportional to the velocity  $v$  of the object:

$F_f = -cv$ , where  $c$  is called the viscous damping coefficient.

Balance of forces (Newton's second law) for damped harmonic oscillators is then

$$F = -kx - c \frac{dx}{dt} = m \frac{d^2x}{dt^2} \dots \dots \dots \text{equation (5)}$$

When no external forces are present ((i.e. when  $F = 0$ ) means no sources of external influence such as foreign aid of attack either in terms of manware, arms, funding)), this can be rewritten into the form

$$\frac{d^2x}{dt^2} + 2\zeta\omega_0 \frac{dx}{dt} + \omega_0^2 x = 0, \dots \dots \dots \text{equation (6)}$$

where,

$$\omega_0 = \sqrt{\frac{k}{m}}$$

is called the 'undamped(uncontrolled crisis system) angular frequency of the oscillator' and

$$\zeta = \frac{c}{2\sqrt{mk}}$$

is called the 'damping (controlling crisis system)ratio'.

Step-response of a damped harmonic oscillator; curves are plotted for three values of

$$\mu = \omega_1 = \omega_0 \sqrt{1-\zeta^2} \dots \dots \dots \text{equation (7)}$$

Time is in units of the decay time  $\tau = 1/(\zeta\omega_0)$ .  $\dots \dots \dots \text{equation (8)}$

The value of the damping ratio  $\zeta$  critically determines the behaviour of the system. A damped harmonic oscillator can be:

- (i) Overdamped (excessive controlled crisis system) ( $\zeta > 1$ ): The system returns (exponentially decays) to steady state without oscillating. Larger values of the damping ratio  $\zeta$  return to equilibrium slower.
- (ii) Critically damped (well controlled crisis system) ( $\zeta = 1$ ): The system returns to steady state as quickly as possible without oscillating. This is often desired for the damping of systems such as doors.
- (iii) Underdamped (poor controlled crisis system) ( $\zeta < 1$ ): The system oscillates (with a slightly different frequency than the undamped case) with the amplitude gradually decreasing to zero. The angular frequency of the underdamped harmonic oscillator is given by;

$$\omega_1 = \omega_0 \sqrt{1 - \zeta^2}. \dots\dots\dots \text{equation (9)}$$

The Q factor of a damped oscillator is defined as

$$Q = 2\pi \times \frac{\text{Energy stored}}{\text{Energy lost per cycle}}. \dots\dots\dots \text{equation (10)}$$

$$Q = \frac{1}{2\zeta}.$$

$Q$  is related to the damping ratio by the equation

**Driven harmonic oscillators**

When external force is involved in a crisis situation is called driven harmonic oscillators. That is the driven harmonic oscillators are damped oscillators (controlled crisis system) further affected by an externally applied force  $F(t)$ .

Newton's second law takes the form

$$F(t) - kx - c \frac{dx}{dt} = m \frac{d^2x}{dt^2}. \dots\dots\dots \text{equation (11)}$$

It is usually rewritten into the form

$$\frac{d^2x}{dt^2} + 2\zeta\omega_0 \frac{dx}{dt} + \omega_0^2 x = \frac{F(t)}{m}. \dots\dots\dots \text{equation (12)}$$

This equation can be solved exactly for any driving force, using the solutions  $z(t)$  which satisfy the unforced equation:

$$\frac{d^2z}{dt^2} + 2\zeta\omega_0 \frac{dz}{dt} + \omega_0^2 z = 0, \dots\dots\dots \text{equation (13)}$$

and which can be expressed as damped sinusoidal oscillations (controlled complex crisis),

$$z(t) = Ae^{-\zeta\omega_0 t} \sin \left( \sqrt{1 - \zeta^2} \omega_0 t + \phi \right), \dots\dots\dots \text{equation (14)}$$

in the case where  $\zeta \leq 1$ .

The amplitude  $A$  and phase  $\phi$  determine the behaviour needed to match the initial conditions.

**Step input or response**

In the case  $\zeta < 1$  and a unit step input with  $x(0) = 0$ :

$$\frac{F(t)}{m} = \begin{cases} \omega_0^2 & t \geq 0 \\ 0 & t < 0 \end{cases} \dots\dots\dots \text{equation (15)}$$

the solution is:

$$x(t) = 1 - e^{-\zeta\omega_0 t} \frac{\sin(\sqrt{1-\zeta^2}\omega_0 t + \varphi)}{\sin(\varphi)}, \dots\dots\dots\text{equation (16)}$$

with phase  $\varphi$  given by

$$\cos \varphi = \zeta.$$

The time an oscillator needs to adapt to changed external conditions is of the order  $\tau = 1/(\zeta\omega_0)$ . In physics, the adaptation is called relaxation, and  $\tau$  is called the relaxation time. In electrical engineering, a multiple of  $\tau$  is called the *settling time*, i.e. the time necessary to ensure the signal is within a fixed departure from final value, typically within 10%. The term *overshoot* refers to the extent the maximum response exceeds final value, and *undershoot* refers to the extent the response falls below final value for times following the maximum response.

**In the case of a sinusoidal driving force** (a cause complex crisis):

$$\frac{d^2x}{dt^2} + 2\zeta\omega_0 \frac{dx}{dt} + \omega_0^2 x = \frac{1}{m} F_0 \sin(\omega t), \dots\dots\dots\text{equation (17)}$$

where  $F_0$  is the driving amplitude and  $\omega$  is the driving frequency for a sinusoidal driving mechanism. This type of system appears in AC driven RLC circuits (resistor-inductor-capacitor) and driven spring systems having internal mechanical resistance or external air resistance.

The general solution is a sum of a transient solution (short duration solution) that depends on initial conditions,

and a steady state that is independent of initial conditions and depends only on the driving amplitude  $F_0$ , driving frequency,  $\omega$ , undamped (uncontrolled) angular frequency  $\omega_0$ , and the damping ratio  $\zeta$ .

The steady-state solution is proportional to the driving force with an induced phase change of  $\phi$ :

$$x(t) = \frac{F_0}{mZ_m\omega} \sin(\omega t + \phi) \dots\dots\dots\text{equation (18)}$$

where

$$Z_m = \sqrt{(2\omega_0\zeta)^2 + \frac{1}{\omega^2} (\omega_0^2 - \omega^2)^2}$$

is the absolute value of the impedance or linear response function and

$$\phi = \arctan \left( \frac{\omega_0^2 - \omega^2}{2\omega\omega_0\zeta} \right)$$

is the phase of the oscillation relative to the driving force, if the arctan value is taken to be between -180 degrees and 0 (that is, it represents a phase lag, for both positive and negative values of the arctan's argument).

For a particular driving frequency called the resonance, or resonant frequency

$$\omega_r = \omega_0 \sqrt{1 - 2\zeta^2}, \dots\dots\dots\text{equation (19)}$$

the amplitude (for a given  $F_0$ ) is maximum.

This resonance effect only occurs when  $\zeta < 1/\sqrt{2}$ , i.e. for significantly underdamped systems.

For strongly underdamped systems the value of the amplitude can become quite large near the resonance

frequency.

### 7. Short Term Solutions to Crisis Situation

Application of short term solutions to crisis situation is called transient solutions. The transient solutions are the same as the unforced ( $F_0 = 0$ ) damped harmonic oscillator (control crisis system) and represent the systems response to other events that occurred previously. The transient solutions typically die out rapidly enough that they can be ignored.

A parametric oscillator is a driven harmonic oscillator in which the drive energy is provided by varying the parameters of the oscillator, such as the damping or restoring force. A familiar example of parametric oscillation is "pumping" on a playground swing. A person on a moving swing can increase the amplitude of the swing's oscillations without any external drive force (pushes) being applied, by changing the moment of inertia of the swing by rocking back and forth ("pumping") or alternately standing and squatting, in rhythm with the swing's oscillations. The varying of the parameters drives the system. Examples of parameters that may be varied are its resonance frequency  $\omega$  and damping  $\beta$ .

*Universal oscillator equation is given as;*

$$\frac{d^2q}{d\tau^2} + 2\zeta \frac{dq}{d\tau} + q = 0 \quad \dots\dots\dots \text{equation (20)}$$

since all second order linear oscillatory systems can be reduced to this form. This is done through nondimensionalization.

If the forcing function is  $f(t) = \cos(\omega t) = \cos(\omega t_c \tau) = \cos(\omega \tau)$ , where  $\omega = \omega t_c$ , the equation becomes,

$$\frac{d^2q}{d\tau^2} + 2\zeta \frac{dq}{d\tau} + q = \cos(\omega \tau). \quad \dots\dots\dots \text{equation (21)}$$

The solution to this differential equation contains two parts, the "transient" and the "steady state".

Transient solution based on solving the ordinary differential equation is for arbitrary constants  $c_1$  and  $c_2$

$$q_t(\tau) = \begin{cases} e^{-\zeta\tau} (c_1 e^{\tau\sqrt{\zeta^2-1}} + c_2 e^{-\tau\sqrt{\zeta^2-1}}) & \zeta > 1 \text{ (overdamping)} \\ e^{-\zeta\tau} (c_1 + c_2\tau) = e^{-\tau} (c_1 + c_2\tau) & \zeta = 1 \text{ (critical damping)} \\ e^{-\zeta\tau} [c_1 \cos(\sqrt{1-\zeta^2}\tau) + c_2 \sin(\sqrt{1-\zeta^2}\tau)] & \zeta < 1 \text{ (underdamping)} \end{cases} \quad \dots\dots \text{equation (22)}$$

The transient solution is independent of the forcing function.

To obtain steady-state solution, apply the "complex variables method" by solving the auxiliary equation below and then finding the real part of its solution:

$$\frac{d^2q}{d\tau^2} + 2\zeta \frac{dq}{d\tau} + q = \cos(\omega\tau) + i \sin(\omega\tau) = e^{i\omega\tau}. \quad \dots\dots\dots \text{equation (23)}$$

Supposing the solution is of the form

$$q_s(\tau) = Ae^{i(\omega\tau+\phi)}. \quad \dots\dots\dots \text{equation (24)}$$

Its derivatives from zero to 2nd order are

$$q_s = Ae^{i(\omega\tau+\phi)}, \quad \frac{dq_s}{d\tau} = i\omega Ae^{i(\omega\tau+\phi)}, \quad \frac{d^2q_s}{d\tau^2} = -\omega^2 Ae^{i(\omega\tau+\phi)}. \quad \dots\dots\dots \text{equation (25)}$$

Substituting these quantities into the differential equation gives

$$-\omega^2 A e^{i(\omega\tau+\phi)} + 2\zeta i\omega A e^{i(\omega\tau+\phi)} + A e^{i(\omega\tau+\phi)} = (-\omega^2 A + 2\zeta i\omega A + A) e^{i(\omega\tau+\phi)} = e^{i\omega\tau} \dots \text{equation (26)}$$

Dividing by the exponential term on the left results in

$$-\omega^2 A + 2\zeta i\omega A + A = e^{-i\phi} = \cos \phi - i \sin \phi. \dots \text{equation (27)}$$

Equating the real and imaginary parts results in two independent equations

$$A(1 - \omega^2) = \cos \phi \quad 2\zeta\omega A = -\sin \phi.$$

Squaring both equations and adding them together gives

$$\left. \begin{aligned} A^2(1 - \omega^2)^2 &= \cos^2 \phi \\ (2\zeta\omega A)^2 &= \sin^2 \phi \end{aligned} \right\} \Rightarrow A^2[(1 - \omega^2)^2 + (2\zeta\omega)^2] = 1. \dots \text{equation (28)}$$

Therefore,

$$A = A(\zeta, \omega) = \text{sign} \left( \frac{-\sin \phi}{2\zeta\omega} \right) \frac{1}{\sqrt{(1 - \omega^2)^2 + (2\zeta\omega)^2}}. \dots \text{equation (29)}$$

Compare this result with the theory section on resonance, as well as the "magnitude part" of the RLC circuit. This amplitude function is particularly important in the analysis and understanding of the frequency response of second-order systems.

To solve for  $\phi$ , divide both equations to get

$$\tan \phi = -\frac{2\zeta\omega}{1 - \omega^2} = \frac{2\zeta\omega}{\omega^2 - 1} \Rightarrow \phi \equiv \phi(\zeta, \omega) = \arctan \left( \frac{2\zeta\omega}{\omega^2 - 1} \right). \dots \text{equation (30)}$$

This phase function is particularly important in the analysis and understanding of the frequency response of second-order systems.

Full solution can be obtained by combining the amplitude and phase portions results in the steady-state solution

$$q_s(\tau) = A(\zeta, \omega) \cos(\omega\tau + \phi(\zeta, \omega)) = A \cos(\omega\tau + \phi). \dots \text{equation (31)}$$

The solution of original universal oscillator equation is a superposition (sum) of the transient and steady-state solutions

$$q(\tau) = q_t(\tau) + q_s(\tau). \dots \text{equation (32)}$$

### 8. Aim of the Research

The aim of this paper is to seek ICT tools solution to crime and insurgence attack in Nigeria by providing a broad view of the PSCS, PSN and NSIC and some ways that ICT-based technologies can assist security agencies in been more efficient and effective in their operations for national development.

### 9. Research Objectives

The research objectives are;

- (i) To introduce a new technique for tackling crime such as public safety networks (PSNs) and National Security Information Centre(NSIC) and to revitalised the existing public security communications system (PSCS), so as to produce a safety environment that is devoid of frequent attacked by insurgence,
- (ii) To create an improved public security communications system (PSCS) and public safety networks (PSNs) by involving public and using ICT tools in information gathering,



- (iii) To suggest a national information database such as National Security Information Centre (NSIC) that have every citizen and foreigners details,
- (iv) To recommend methods for a better security in tackling insurgency in Nigeria.

### 10. Statement of Research Problem

Terrorism as unleashed by Boko Haram has primarily targeted government security agencies most especially the police, public buildings, churches and markets. About 50,000 lives has been loss and properties worth of 160billion naira of Nigeria currency about (1billion US dollars) has been loss as a result of the attacked. With over five decades of nationhood, Nigeria has never witnessed the kind of insurgency that has engulfed the country in the past five years. The post-presidential election of 2011 and the concomitant uproar it generated most especially in the northern part of the country fuelled the upsurge of insurgency. The problem is reflecting religion, political, economic, social and cultural realities in Nigeria. This national insecurity has led to the postponement of democratic election the year 2015. The Federal Government of Nigeria did not initially; take serious interest in the activities of the sect until 2009 when intelligence reports showed that the group had the potential of being dangerous to the general safety and welfare of Nigerian’s citizens. Although the group was labelled as a terrorist organization in 2011 after the bombing of the United Nations headquarters in Abuja, the actual classification of the group as a terrorist group associated with Al-Qaida did not occur until November 2013 by the United States government.

**Bayes’ theorem** “provides a means of changing one’s knowledge about an event in the light of new evidence related to the event”. It is represented as:

$$P_r(A/E) = P_r(A) * P_r(E/A) / P_r(E) \dots\dots\dots \text{equation (33)}$$

where

$$P_r(A) \text{ is the prior probability} \dots\dots\dots \text{equation (34)}$$

$$P_r(A/E) \text{ is the posterior probability} \dots\dots\dots \text{equation (35)}$$

**Note:**  $P_r(E/A) / P_r(E)$  is the relative likelihood

In a complex multi-cultural society such as a Nigeria, the possibilities of a crisis occurrence may be so involved that a systematic scheme for identifying all the potential crisis situation and their respective consequences is necessary.

The probability of a danger, P(E) is calculated by:

$$P(E) = 1 - (1-p_1)(1-p_2)\dots\dots(1-p_k) \dots\dots\dots \text{equation (36)}$$

Therefore, the crisis in the North Eastern States has become so complex but very clear solution which can be related to a complex multi-cultural society which provides a means of changing one’s knowledge about the event in the light of new evidence related to the event”.

### 11. Significant of Study

This research is worth conducting because of the believe crises or terrorism attack usually have on people, most especially the vulnerable (e.g. children and women), this we viewed from social-political and economic perspectives.

The emergence of killers like Islamic fanatics “Boko Haram and Fulanis herdsmen” has rendered the affected states physically bad. Therefore, the ugly situation has call for the need of introducing an early warning signal or alert communication to the community that is about to be in crisis so as to take adequate precaution. The role of ICT in tackling crime in modern times can be study and applied in this case just as is been done in the western world in tackling crimes. Surveillance camera has been one of the most visible in modern cities that are used to address criminality. The United Kingdom is ringed with a total of 1.85 million close circuit television cameras (CCTV). The city of London alone boasts of 422,000 CCTV cameras with a camera assigned to every 14 persons.

The importance of Public Safety Networks (PSNs) system can be seen from the benefits and this include;

- Time cost reduce to averting crisis
- (ii) Easy access to information and communication thereby averting crisis
- (iii) Online fast and secure crisis management
- (iv) Security improvement access to protection
- (v) Organizational efficiency improvement for the security offices
- (vi) Solution for effective and efficient crisis management strategies
- (vii) Less energy used in averting crisis
- (viii) Time spent reduce to averting crisis
- (ix) Live saving
- (x) Properties preserved

## 12. Research Questions

In order to fulfill the purpose of this study the following research questions (RQ) have been formulated:

RQ1: How can different type of terrorism be described?

RQ2: How can terrorism communication strategies used to handle a terrorism be described?

The research questions include criteria for use of ICT tools, Computerization, Networking and Internet such as;

1. What is existing system of public security communications system (PSCS) and public safety networks (PSNs)?
2. Can the problem be solved using ICT tools such as GSM, Camera, Satellite, Radio, CCTV, Computer, networking and Internet?
3. It is effective?
4. It is going to be efficient?
5. It is going to be reliable?

### Other relevant questions include;

1. What actions have been taken by the government to solve community crisis?
2. What programs has the government introduced to provide faster access to communication and information?
3. What are the skills, beliefs and attitudes of the people toward introduction of ICT tools such as GSM, radio, camera, CCTV, satellite and computer based Public Security Communications System (PSCS) and Public Safety Networks (PSNs) system?

Also, in trying to find answers to the research questions, hypothesis testing is proposed.

## 13. Research Hypotheses

The Hypotheses of the study is taken from technology acceptance model (TAM) is an information systems theory that models how users come to accept and use a technology. The model suggests that when users are presented with a new technology, a number of factors influence their decision about how and when they will use it, notably:

Perceived usefulness (PU) - This was defined by Fred Davis as "the degree to which a person believes that using a particular system would enhance his or her job performance".

Perceived ease-of-use (PEOU) - Davis defined this as "the degree to which a person believes that using a particular system would be free from effort" (Davis 1989).

The TAM has been continuously studied and expanded-the two major upgrades being the TAM 2 (Venkatesh & Davis 2000 & Venkatesh 2000) and the Unified Theory of Acceptance and Use of Technology (or UTAUT, Venkatesh et al. 2003). A TAM 3 has also been proposed (Venkatesh & Bala 2008).

Several researchers have replicated Davis's original study (Davis 1989) to provide empirical evidence on the relationships that exist between usefulness, ease of use and system use (Adams, Nelson & Todd 1992; Davis 1989; Hendrickson, Massey & Cronan 1993; Segars & Grover 1993; Subramanian 1994; Szajna 1994). Much attention has focused on testing the robustness and validity of the questionnaire instrument used by Davis. TAM lies in the hypothesis that intention to use a system is determined by two variables:

- (i) perceived usefulness and,
- (ii) perceived ease of use.

Perceived usefulness is defined as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989). While perceived ease of use is defined as "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989).

According to Venkatesh and Davis (2000), TAM theories that perceived usefulness and ease of use mediate the relationship between external variables, such as system characteristics, development process, training, and intention to use a system. The Figure 3 presented TAM, version 1. (Davis 1989).

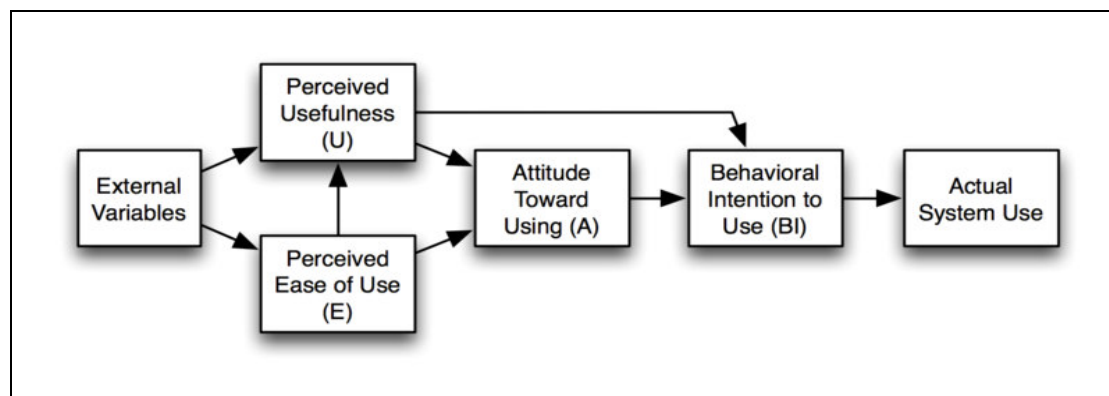


Figure 3. The Technology Acceptance Model, version 1. (Davis 1989)

As shown in Figure 1, perceived usefulness and ease of use are hence user's beliefs on information technology and therefore form user's attitude toward technology which will, in turn, predict acceptance. The Hypothetical statements are as follows:

H1: The Application of ICT tools in tackling crime is a way of reducing crime rate

H2: Application of ICT tools in the fight against crime is an effective and efficient way of developing superior strategy to reduce the menace

H3: Government is aware of the importance of ICT and criticality of crime and terrorist

H4: Application of ICT tools in the fight against crime would improve security operational efficiency of the personnel

H5: Government's need ICT knowledge and today's security is based on managing ICT knowledge resources

H6: Application of ICT tools in the fight against crime is a way of creating intellectual approach as a solution advantage for crime and terrorist free society

H7: Application of ICT tools in the fight against crime and terrorism could help security operatives to deal with skills of crime more effectively and efficiently

H8: There will be increase in crime and terrorism if supportive modern infrastructure such as ICT tools are lacking

H9: Outsourcing and application of ICT tools will increase crime in the society

#### 14. Limitation of the Study

This research work is limited to developing Public Security Communications System (PSCS) Public Safety Networks (PSNs) and National Security Information Centre (NSIC) system as a means of using secure information to tackle Boko Haram insurgency in the North Eastern Nigeria.

#### 15. Scope/delimitation of the Study

To fulfill the goal, the paper studied behaviour patterns of insurgency techniques, traditional approach and modern approach in tackling terrorism and sample public opinion by questionnaires, results indicate that variables and factors assessed in this study can significantly affect public safety and communication security.

#### 16. Methodology of the Research

There have been various mental methods and approaches employed by the government in tackling the insurgency such as the use of police, military, vigilante and local hunters. Also there have been a lot of seminars and conferences held on security issues on many occasions in Nigeria. The situation can be well tackled through the deployment of ICT, such as the satellite that would produce the desired results." This paper is a proactive study encouraged by the increase in the use of ICT tools in Nigeria as well as restructuring of department of security service (DSS), police and soldiers. The main thrust was aimed at studying modern trends and requirements in Public Security Communications System (PSCS), Public Safety Networks (PSNs) and National Security Information Centre (NSIC) system with a view to understanding the applicability of ICT tools such as Satellite Remote Sensing (SRS) technology to enhance present efforts.

Public Security Communications System (PSCS) is an approach by the federal government towards providing modern infrastructure for public security and e-policing in Nigeria which need revitalization a better efficiency.

Also, government has setup Coalition Emergency Response Subsystem (CERS), which supports the Police call centre for emergency information. This subsystem allows emergency response in emergency situations by emergency services. It provides a national platform for emergency calls by citizens to the Nigeria Police nationwide. Under this subsystem, mobile emergency communication vehicles (ECVs) may be deployed

in emergency situations when commercial communications networks are incapacitated, similarly this aspect need revitalization and transformation for a better efficiency. The new approach are;

(i) Public Safety Networks (PSNs) this is an ICT network that can be establish by the authorities to both warn and prepare the population for an imminent danger, or to provide support during the crisis and normalization phases. PSNs have the fundamental role of providing communication and coordination for emergency operations. Many of the problems of the PSCS field come from the heterogeneity of systems and agencies involved at the crisis site and from their mobility patterns within the disaster or crisis area.

(ii) National Security Information Centre (NSIC) this is an ICT network that provide immediate information or data that can be gotten from the public which can serve as a database for immediate response to crisis situation. This is quite different from the approach by government through “National Information Centre”, which comprises of media and security agencies only.

### 17. Related Work

Some related previous works include: “Using ICT to Fight Crime -A Case of Africa”[10],“The Role of ICT in Tackling Security Challenges in Nigeria”[11],“The Caribbean ICT Research Programme”[12],“Megacity Challenges Public Safety and Possible ICT Solutions- A Citizen Centered Approach”[13]. Others are “Global Response to Cyber Threats [14]”, A Computer-Based Security Framework for Crime Prevention in Nigeria”[15], and “Effectiveness of Information and Communication Technology”[16]. Some of these papers have emphasized ICT solution to crime.

### 18. Research Design/Approach

Here are some ways that ICT-based technologies can assist security agencies in achieving more efficiency and effectiveness in their operations.

(1) Surveillance: Surveillance is a deliberate system of keeping a close watch on the behaviours or activities of persons, groups, organisations and institutions suspected of doing something illegal or capable of causing a breach of security by government’s security agencies.

This could be done electronically with *closed circuit television* cameras or interception of electronically transmitted information (such as Internet traffic or phone calls) or by means of low-technology methods such as human intelligence agents and postal interception.

Other means include: surveillance cameras, social network analysis, biometric surveillance, data mining and profiling, corporate surveillance, satellite imagery, radio-frequency identification and geo-location devices to mount surveillance on suspected targets.

(2) Intelligence Gathering: Intelligence gathering helps security agencies to keep tabs on the activities of suspected groups, organisations or persons likely to breach the peace. Today, such ICT tools as the internet, mobile telephony system, social media networks and the media have become veritable platforms for intelligence gathering efforts of our security agencies, so long as they observe the ethics of using these technologies for intelligence gathering purposes.

(3) Communication: Intercepting communication between terrors and terror groups and enhancing intelligence sharing and other collaborative measures between security agencies is now absolutely possible through ICT tools. We now have electronic devices and gadgets with in-built unique identification numbers that makes them electronically traceable regardless of location. So it’s no longer impossible to track communication devices or gadgets used by criminal gangs or groups.

(4) Financing: ICT is a vital tool for tracking, tracing and investigating suspected financial transactions funnelled to criminal activities. With the recent introduction of cash-less society, transactions will be done on electronic platforms where suspicious cash movements can be identified and questioned. This would go a long way in curbing the financing of activities that constitute a threat to national security because no terrorist group or gang can operate without funding.

(5) Coordination: Security agencies can minimise duplication of efforts, guard against the mishandling of information as well as enhance information sharing among them for a better management of our national security through ICT. This involves pulling the nation’s data into a coordinated and centralised database as a proactive means of combating insecurity.

(6) The creation of a Central Intelligence Unit (CIU) or Counter Terrorism Unit (CTU) within arm forces and security agencies with a robust, dynamic, vibrant and updated central database for the country. The centralised database should contain every person’s data and details.

(7) Identification: In advanced countries of the world, birth and death registration, in addition to unifying various identification initiatives, plays significant roles in national security, especially when combined with DNA, facial recognition and finger printing technologies which operate on platforms provided by ICT. That is why it is easier in those climes to easily track down criminals.

(8) Establishment of Integrated Ballistics Information Systems (IBIS)

- (9) Establishment of Traffic Ticketing System (TTIS)
- (10) Establishment of Crime and Information Management System (CIMS)
- (11) Use of Geographic Information Systems
- (12) introduction of Automated Fingerprinting Information Systems (AFIS)
- (13) Provision of Adequate ICT tools: that can be used in tackling crime and insurgency. The channel of communications using ICT tools are computer, internet, mobile phone, close circuit television (CCTV), surveillance cameras, social network analysis, biometry surveillance, data mining, satellite imagery, and IP devices, the satellite.
- (14) Conversion of the National Identification Card (NIC) into an electronic form as well as making all the identification (work ID, school ID, drivers' licence, SIM card registration, National ID etc.) into a single digital electronic form and uploaded on a central database.
- (15) Public enlightenment: Recently, a church in Nigeria unveiled its e-portal system that computerised membership registration and other ancillary services. Managers of this e-portal send regular precautionary SMS alerts that assist members to be at alert and take precautionary measures.
- (16) Sensitisation and advocacy: on security enlightenment issues using ICT-driven solutions, therefore, can play significant roles in tackling insecurity in the country.  
Other non-ICT techniques of fighting the terrorist includes;
- (17) Involvement of public and MDA's: All ministries, departments and agencies of Government must be involve in the fight against crime and terror in Nigeria. Importantly, the ministry like the federal ministry of defence, interior and foreign affairs, communications, information, science and technology. Departments such as Immigration, Custom, Federal Airport Authority, Shippers Council, Nigeria Port Authority and Agencies like the Economic and Financial Crime Commission (EFCC) etc.
- (18) Synergizing with private organization: such as telecommunication industries, banks, mining companies, oil companies, industries and construction companies and ship companies etc. should be vigorously involve in the fight against crime and terror in Nigeria.
- (19) Collaboration with community Leaders: such as Obas, Emirs and settlement leaders at various levels etc., must be part in the fight against crime and terror in Nigeria.
- (20) Involvement of Religious Leaders: such as pastors, reverends, bishop, evangelist and Imams. Should be component in the fight against crime and terror in Nigeria.
- (21) Training/Seminars and Conferences: Public awareness training and security personnel training on security issue should continue on daily basis.
- (22) Media and Press men: should be engage in the fight against crime and terror in Nigeria.
- (23) Adequate legislation: The government of Nigeria should enact law that can punish criminals and make law that can against insurgency attack and criminal activities.
- (24) Prosecution and Judgment: Government should setup task force on crime and security will help in the fight against crime and be ready to pass immediate judgment after prosecution according to law.
- (25) Adequate Funding: The Government at all levels, Federal, State and Local must be ready to release money for funding security issues especially as regards to the tackling of crime and insurgency.
- (26) Controlling Immigrant: The government of Nigeria should build an institution that can redeploy illegal immigrant and stop illegal entry of people into the country. This can be more effective by partnering with neighbouring or boarder countries such as Cameroun, Chad, Niger, Benin and Ivory Coast in a way of building a united and formidable force to fight the insurgent.
- (27) Boarder Collaboration: The government of Nigeria should partner with neighbouring or boarder countries such as Cameroun, Chad, Niger, Benin and Ivory Coast in a way of building a united and formidable force to fight the insurgent.
- (28) International Collaboration: The government of Nigeria should seek assistance of Economic Community of West African States (ECWAS), African Union (AU), United Nations (UN) and Developed Countries to fight the Boko Haram insurgency.

### **19. Type of ICT tools in tackling insurgency**

The table 1 shown the participant responses to the type of ICT tools that could be applying to tackle terrorism, there are one thousand respondents on the effective way to communicate to security agency during crisis or insurgency attack.

Parameters	ICT tools	Frequency	% of the respondent
1	mobile phone	233	23
2	internet	25	3
3	close circuit television (CCTV)	103	10
4	surveillance cameras	101	10
5	social network analysis	80	8
6	satellite imagery	130	13
7	biometry surveillance	71	7
8	IP devices	27	3
9	fax machine	11	1
10	television	86	9
11	radio	120	12
12	data mining	13	1
	<b>Total</b>	<b>1000</b>	<b>100</b>

## 20. Research Hypotheses/Questions Analysis and Results

Results from questionnaire to citizens were designed to find out if the use of ICT tools can reduce insecurity and insurgency attack. Two groups of citizens were interviewed; urban and rural dwellers. The results are given according to the stratification.

Based on the research questions/hypotheses the Tables 2 presents the summary hypotheses analysis and results.

Table 2 Hypothesis Results

Hypothesis	Description	Status	Technique
H1	The Application of ICT tools in tackling crime is a way of reducing crime rate	accepted	Count-procedure Frequency analysis Non-parametric chi-square
H2	Application of ICT tools in the fight against crime is an effective and efficient way of developing superior strategy to reduce the menace	rejected	Count-procedure Frequency analysis Non-parametric chi-square
H3	Government is aware of the importance of ICT and criticality of crime and terrorist	accepted	Count-procedure Frequency analysis Non-parametric chi-square
H4	Application of ICT tools in the fight against crime will not improves security operational efficiency of the personnel	rejected	Count-procedure Frequency analysis Non-parametric chi-square
H5	Government's need ICT knowledge and today's security is based on managing ICT knowledge resources	rejected	Count-procedure Frequency analysis Non-parametric chi-square
H6	Application of ICT tools in the fight against crime is a way of creating intellectual approach as a solution advantage for crime and terrorist free society	Rejected not clearly	Count-procedure Frequency analysis Non-parametric chi-square
H7	Application of ICT tools in the fight against crime could help security operatives to deal with skills of crime more effectively and efficiently	accepted	Count-procedure Frequency analysis Non-parametric chi-square
H8	There will be no increase in crime and terrorism if supportive modern infrastructure such as ICT tools are lacking	rejected	Frequency analysis Non-parametric chi-square
H9	Outsourcing and application of ICT tools will increase crime in the society	accepted not strongly	Frequency analysis Non-parametric chi-square

## 21. Discussion of Hypotheses Results

Statistical results of this study show that security policies are made mainly by legislature and top government functionaries. It also has shown that administration systems, quality control and automation are main domains of security managers. But crime fighting materials and strategy in near future planning. In most advance country ICT tools is mainly intended to speed up traditional human crime management and ICT tools is considered as a system to enable legal security operators to deal with multi-cultural and multi-lingual working contexts and that improves communication and interaction with people and criminal elements. The ICT experts believe that application of ICT tools can lead to a successful tackling of crime in Nigeria due to the efficiency and effectiveness of ICT tools. Statistical and empirical findings of the study also shows that Nigeria crime region or insurgency attack situation faces complexities and difficulties in combating, and the use of gun systems alone seem to not be able to overcome these challenges and therefore more advance systems such as ICT tools, and information database managerial approaches are required. Also it was seen that for Government, outsourcing can be a reliable option to take advantages of ICT tools in presence of financial and technological restrictions. The statistical analysis and empirical findings of this study show that, the overall attitudes and opinions of ICT experts towards the use of ICT tools as a sub-function of an integrated ICT can speed up the critical activities of security and human resource management as the main trigger for utilizing and adopting an ICT tools for crime tackling to reduce crime.

However, findings shown that the ability to communicate and manage a multilingual organizational and environment is the most important operational benefit of a computerized information centre and adoption of ICT tools. This leads to improving external and internal interactions and communications between security personnel, people and government as well as the ability to use information data bases to store and retrieve data. These are the main strategic advantages of a crime free society for security organization in Nigeria. The findings of this study also show that the use of ICT tools in Nigeria is still new and progressive and even some security organizations are not using such systems for their crime monitoring procedures.

More attention needs to be committed by organization, academicians, and practitioners to application of ICT tools as an effective crime monitoring system for all sectors. In addition, there are some useful managerial implications drawn from the study. These will enhance their security decision making and improve the performance and operation of their respective administration from a human resource management perspective and its recruitment sub function. At this time, the society is leaning towards complexity and peoples are encountering many challenges to find peace in the midst of wide range security organization like the Nigeria Security and Civil Defence Corps, Police, Department of State Security and Army. In this case, ICT system can enable human resource managers to analyze crime information database and thereby gain more effective access to criminals.

## 22. Discussion of questionnaire Results

The Figure 3 presents the frequency of respondent to the type of ICT devices that could be applying to tackle terrorism, there are one thousand respondents on the best ICT tools deployment. The result shown that use of mobile phone was favour as the most effective way to communicate to security agency during crisis. Also, the use of satellite imagery, radio, close circuit television (CCTV), surveillance cameras, television and social network analysis are very effective way to communicate in term of crisis. While data mining and fax machine have the least values. That is to say no singular medium can be used as a measure for tackling crime.

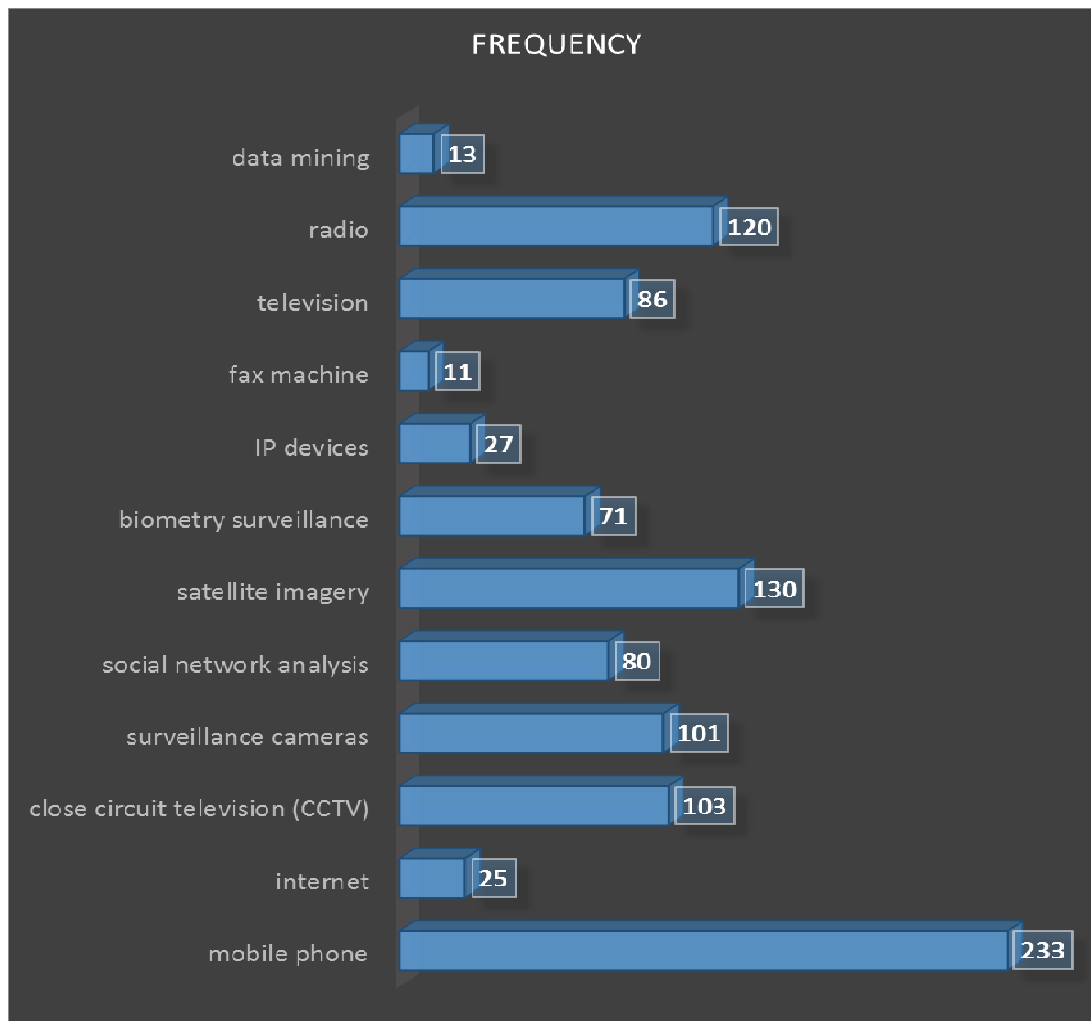


Figure 3: Frequency of respondent to the type of ICT tools

The Figure 4 is the percentages of the respondent's on the type of ICT tools deployable during crisis. The mobile phone constitutes the most respondent with 23%. While the use of satellite imagery score 13%, radio 12%, close circuit television (CCTV) 10%, surveillance cameras 10%, television 9% and social network analysis 8%. This indicates that the participant believe in the use of ICT tools to tackle insurgent like the ravaging Boko-Haram.



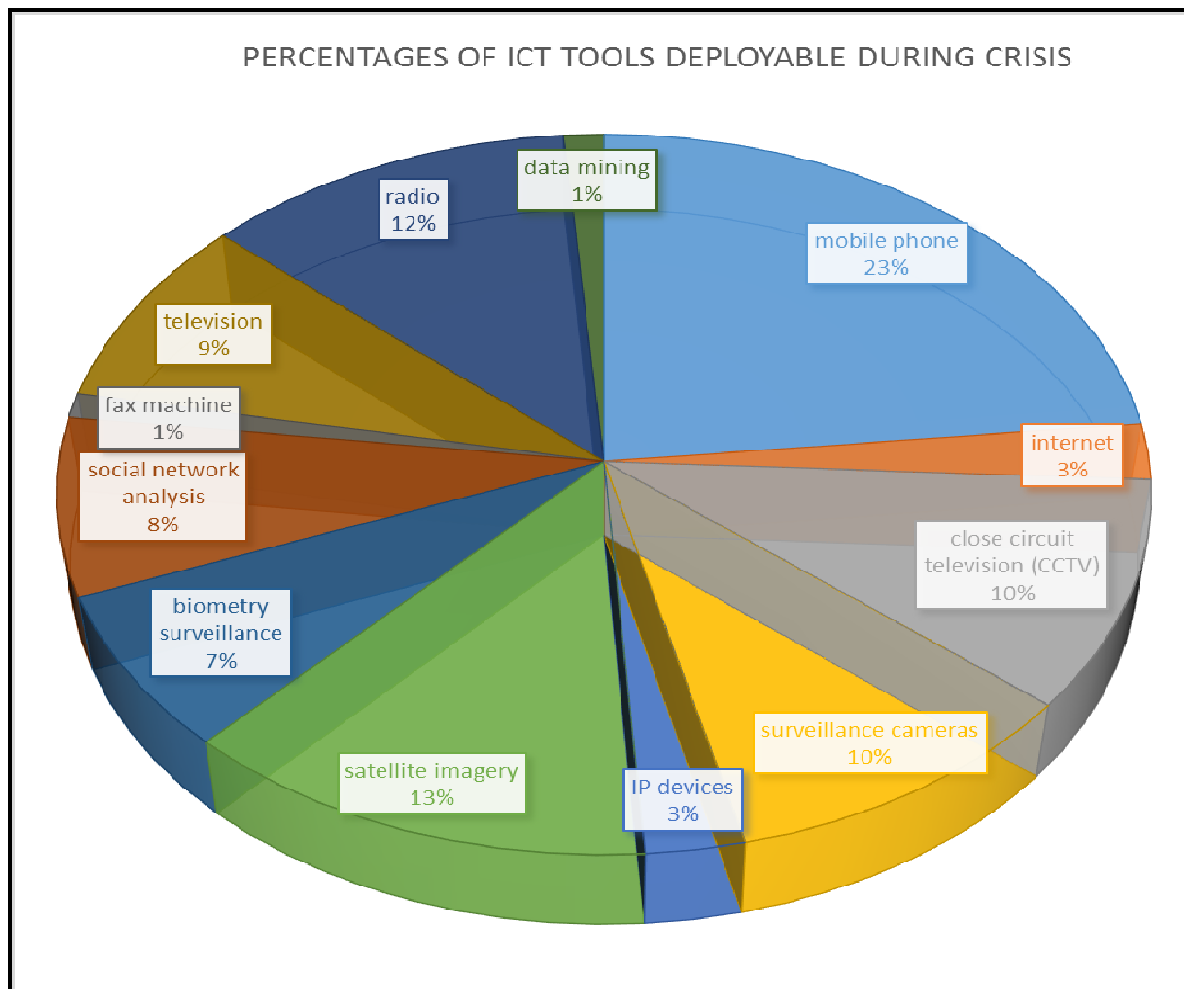


Figure 4: Percentages of type of ICT tools deployable during crisis

### 23. Conclusions

This work focused on introduction of new approaches in the handling of insecurity in Nigeria so as to secure the nation from destroyers of Boko Haram insurgency.

The new approaches includes; public security communications system (PSCS), public safety networks (PSNs), national security information centre (NSIC) system and techniques for tackling for Boko Haram insurgency. It is the perspective of this that the work make attempt to improve and enhance that is of national challenge and that is what have been presented for appropriate safe- guide measure.

With this introduction of public security communications system (PSCS), public safety networks (PSNs) and national security information centre (NSIC) system, the north eastern states communities crisis can be effectively and efficiently manage and completely eliminated.

The participants highlighted the complex and centralised crisis management system for the new digital system in the crisis states. They noted that the procedure involved distribution of information identify the need for training in the new system. The quick access to information can be achieved within seconds.

This issue is revealed by some extent that perceived given of information and perceived ease of information can contribute to informal or users satisfaction. User perception of different types of values can also be further understood by the future study approach.

### 24. Recommendations

- (i) Public awareness training and security personnel training on security issue should continue on daily basis.
- (ii) Analyses of these trends leads us the following recommendation: greater priority must be given to crime prevention in public safety policies:

Safety and prevention strategies, as defined by the United Nations, must constitute public policies in and of themselves, and not be annexed to other policies. They must benefit from adequate and specific resources both in terms of funding and governance, management capacities, follow-up, and evaluation.

Federal, State and Local agencies that are directly connected to the needs of crisis communities need to be sustain, financially empower and power manage.

It is important to include security studies and disaster management in the country's education curriculum.

## 25. Suggestions for Further Research

This paper is based on a scientific study and could be used as a base for further research since national security information centre can be improved upon and the technology of data is still evolving, it would be a good idea for further research to be carried out on

(i) Both public safety networks (PSNs) and national security information centre (NSIC) system can be further research upon before its implementation.

(ii) Since we could not gather enough data to support all our hypotheses, we propose that further research should be done in the area of high rate of data transfer and communication.

(iii) Moreover, further studies can be conducted as a complement to this paper or as a follow-up on this work and it would be more appropriate; to find out whether the factors proposed in this paper, actually influenced data security.

(iv) We here by suggest a research on the security issues to data communication.

(v) There is need for more research work into the field of public safety networks for a better secure future.

(vi) Research can be conducted into development of an algorithm that can hide information through communication channel in crisis situation.

(v) Furthermore, investigators can work on performing transnational studies amongst causes of insurgency in Nigeria and other countries to enable understanding and analyzing the role of international security and also international competition of firms based on labor across a broader geographical scope.

Finally, no nation can progress in a state of insecurity. Progress comes when economic activities take place in an environment of safety. Therefore, every nation including Nigeria must include national security as one of their enduring interest so as to create enabling environment for economic, political, and social activities to thrive. Nigeria national security must be an issue for every Nigerian. This is because, a state of insecurity can hamper Nigeria vision becoming one of the leading 20 nations of the world by the year 2020 which is few years away.

## 24. Acknowledgments

We thank Department of Physics, Nigerian Defence Academy (NDA) Kaduna, Department of Mathematics Ahmadu Bello University Zaria, Energy Commission of Nigeria (ECN) and Department of Mathematics Nasarawa State University Keffi Nigeria for the material support during the research work. The authors would like to express profound gratitude to anonymous reviewers for their valuable comments and suggestions that improve the presentation of this paper.

## References

- [1] Premium Times 2015. Boko Haram: Over 1,000 civilians killed since January – Human Rights Watch. Published by: Premium Times March 26 2015 Nigeria. Available at: <http://www.premiumtimesng.com/news/headlines/179146-boko-haram-over-1000-civilians-killed-since-january-human-rights-watch.html>
- [2] Guardian 2014. Boko Haram insurgents reportedly invaded Chibok in a convoy of vehicles on April 14 2014. Published by: Guardian Newspaper April 15 2014 Nigeria. Available at: <http://pulse.ng/local/boko-haram-terrorists-launch-another-attack-on-chibok-id3557428.html>
- [3] International Business Times 2015. Boko Haram Attacks Killed Over 1,000 Civilians In 2015, Human Rights Watch Says 27 March 2015 Nigeria. Available at: <http://www.ibtimes.com/boko-haram-attacks-killed-over-1000-civilians-2015-human-rights-watch-says-1860158>
- [4] The Sun News 2014. ICT 'll tackle Boko Haram. opening ceremony of the 25th annual national conference of the Nigeria Computer Society at Enugu. Published by: The Sun Newspaper - Sunday, 27 July 2014
- [5] Insecurity 2014. Information Technology CWG, Huawei Canvass IP Surveillance  
Published By: The Punch Newspaper » - Sunday, 4 May, 2014  
[http://www.cwlgrou.com/ITGraffiti-Week\\_5th\\_9th\\_May\\_2014](http://www.cwlgrou.com/ITGraffiti-Week_5th_9th_May_2014)
- [6] A.B Okauru 2013. Information Communication Technology and National Security in Nigeria. Published by: Punch Newspaper July 28, 2013. Available at: <http://www.punchng.com/business/ict-clinic/security-challenges-what-can-ict-do/>
- [7] Thisday 2013. Addressing National Security Challenges with Technology Tools. Published by: Thisday Newspaper Saturday September 12, 2013 Nigeria. Available at: <http://www.thisdaylive.com/articles/addressing-national-security-challenges-with-technology-tools/158831/>

- [8] He made this statement last week in Enugu during the opening ceremony of the 25th annual national conference of the. The post 'ICT tackle Boko Haram' appeared first on The Sun News Published by: The Sun News - Sunday, 27 July.
- [9] Alexandros Paraskevas 2006. Crisis management or crisis response system. A complexity science approach to organizational crises. Department of Hospitality, Leisure and Tourism Management, Business School, Oxford Brookes University, Oxford, UK.
- [10] Henry Osborn Quarshie 2014. Using ICT to Fight Crime -A Case of Africa  
MBA (MIS) pg. Cyber law Lecturer regent university college of science & technology, Accra, Ghana
- [11] Habibat Ndanusa The Role of ICT in Tackling Security Challenges in Nigeria  
Lecturer at Yusufu Bala Usman College of Legal and General Studies
- [12] Michele Thomas . Networks for Development: The Caribbean ICT Research Programme Rapid Response Research Project . Draft Policy Framework Caribbean Telecommunications Union Collaboration Policy for Functional Cooperation through ICT, in the Area of Crime and Security. Vol. 5, No. 1 January 2014 ISSN 2079-8407 Journal of Emerging Trends in Computing and Information Sciences ©2009-2014 CIS Journal.
- [13] Dhanfia Habeeb Rahman 2013. Megacity Challenges Public Safety and Possible ICT Solutions- A Citizen Centered Approach. University of Uppsala, Department of Information Technology
- [14] Saulius Pakalniškis 2012. Global Response to Cyber Threats. Leiden University
- [15] G.O.Ogunleye1 et al. (2011). A Computer-Based Security Framework for Crime Prevention in Nigeria.
- [16] Ibikunle Frank and Adefihan Binpe (2014). Effectiveness of Information and Communication Technology (ICT) in Policing in Nigeria. Scottish Journal of Arts, Social Sciences and Scientific Studies. Available at: <http://scottishjournal.co.uk>

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:

<http://www.iiste.org>

### CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

**Prospective authors of journals can find the submission instruction on the following page:** <http://www.iiste.org/journals/> All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

### MORE RESOURCES

Book publication information: <http://www.iiste.org/book/>

Academic conference: <http://www.iiste.org/conference/upcoming-conferences-call-for-paper/>

### IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digital Library, NewJour, Google Scholar

