ISSN:0975-9646

ICT And National Security in Developing and Underdeveloped Countries – The Good, The Bad and The Ugly: A Case Study of Nigeria's Cyberspace

Emmanuel C. Ogu[#], Oyeyinka D. Oyerinde[*]

[#]*Department of Computer Science and Information Systems, Babcock University*
Ilishan-Remo, Ogun State, Nigeria

[*]*Corporate Information Systems, ICT Directorate, University of Jos*
Jos, Plateau State, Nigeria

***Abstract*— Following the dawn of the Information Age, Computers and the Technologies that power them have been proven a double-edged sword with the potential for both good and evil – depending on how much the user(s) can harness them in either direction. On one end of the stick, we seem doused by the development of sophisticated devices and gadgets to assuage our growing need for communication and connectivity and also to combat internet and electronic-related/fostered crimes and the criminals that perpetrate them; while on the other end, we wrestle with the fact that electronic Crimes are becoming more popular, leaving in their wake much more devastating effects than it did in preceeding years. The ICT devices and equipment that are employed right from planning to execution of such and other (similar) crimes are worrisomely becoming *more common, less expensive and more sophisticated* over the years – a nagging fear that some of the most-potent devices are becoming more readily available, more affordable and more devastating as the peace and security of our nations decline before our very eyes with helpless imminence. It is true that a preponderance of the causes of the bane of terrorism and violence, amongst other challenges that befall nations (such as ours) glaringly stem from sources that are more far-reaching; the untold complementary reality, however, is that the propellants of these vices are the devices and equipment (ranging from Mobile Phones and Tablets to GPS and tracking devices, Computers, surveillance equipment and the Internet) that are put further within reach of the citizenry every day and fostered towards negative causes by poor administration and gross mismanagement especially in underdeveloped and developing nations. This recent tide necessitates an urgency to review the concept of Information and Communication Technology and its impact on our National Security for good and otherwise and appraise its contributions in holistic ramifications so as to determine whether our nations are, in essence, leveraging on its advantages or being plagued by its disadvantages.**

In light of this, this research creates an exposé into the facets of the capabilities of Information and Communication Technology – the good, the bad and the ugly; identifying some of the security challenges that have and could be linked causatively to ICT infrastructure and some possible solutions – "what we have" and "what we need", in relation to the growing concerns of National Security; with a focus on citing and analysing situations, especially those that exist in the Nigerian context wherever sources exist and are verifiable.

***Keywords*— Information and Communication Technology (ICT), Developed Countries, Developing Countries, Underdeveloped Countries, International Standards Organization (ISO), Database Management Systems (DBMSs).**

I. INTRODUCTION

ICT (Information and Communication Technology) is a widely defined term that has several meanings across different sectors. Though, essentially, it is used as an umbrella term to refer to the use of communication devices (such as radio and cellular devices, satellite devices and channels, computers, amongst others.) and utilities (programs) to manage information (acquisition, dissemination, processing, storage and retrieval) [3].

In lay terms, National Security could refer to a state of absence of everything and anything that could be a threat to peace, progress, development and tranquillity within a society [7].

With the dawn of the Information Age at about the beginning of the 20th Century, Information and Communication Technology has become a force to reckon with; and over the years, the world has seen a progressive shift from a time when computers and other (radio and cellular) communication devices remained in the exclusive domain of the rich and influential – people who had the financial capability to procure, maintain and sustain these devices – to a time when the average citizen can in reality, possess these devices and manage and utilise them within fair capacities. This shift has brought with it numerous benefits, some of the most popular being that information has become more easily accessible and transmissible across the various societal classes; also, development has been fostered greatly in various societies through the aid of some of the various utilities provided by ICT for Advertising, Marketing and Sales, Management and Administration, Strategizing and Prospecting, Consultancy, Construction, Education and Learning, to mention but a few.

With this shift also, and the advent of the digital (paperless) age of the 21st Century, more concerns have been raised over the security of digital Information especially those that rely on various communication media and networks (such as the Internet) for transmission. The volume of computerized data that is stored and transmitted remain ever increasing in direct proportion with the value (financial, political or otherwise) that could be attached to such stored data. The question of "how secure can my (digital) data / information possibly be, whether I'm transmitting it or not?" has become more pertinent down through the years; a pertinence that has been cast primarily from hard lessons learnt from events of devastating consequences that followed the compromise of highly classified information; one of the most recent and popular being a data leak on Google's Servers during the last quarter of the year 2012 that resulted in the breach of highly sensitive information and a loss of about 22 billion dollars of Google's stock value [2].

As ICT became more closely linked with business successes, politics and national development over the years, it became a very attractive target for malicious hack attacks, not only from outside but from within; [4] and a very potent tool that could be channelled at bringing down critical business infrastructure and compromising national security, progress and development by lowering the competitive edge of many business and organizations in the World Market as can be seen in the histories of Microsoft and Google Corporations over last decade and by fostering violence, terrorism and other vices that hamper progress and national development respectively.

Thus, ICT has consistently been proven a powerful double-edged sword with a capability for both overwhelming good and devastating evil; all depending on the skills and values of the user(s) in harnessing its powers in either or both directions.

II. Past Related Researches

Ibrahim Saleh carried out a research with a goal to help emphasize the need to improve the current media governance and address vital issues of conflict and violence as affecting African Nations, which are permanently on record; creating a better understanding of how ICT could help address issues of conflict, peace and security, and a new media discourse that addresses these topics with a focus societal development and enhancing environmental quality in Africa [8]. In 2010, a research paper was presented by Abdul-Hakeem B.D. Ajijola at the eNigeria Conference held in Abuja, Nigeria. The paper titled, *"The role of ICT Deployment for National Security"* emphasized the National Security Policy Formulation Process, ICT as a tool for knowledge and mass mobilisation and some solutions to problems in ICT which could be implemented at the Executive, Legislative and Judiciary Levels. In March 2012, stakeholders in information technology and defence met in Nigeria to explore ways by which information technology could be harnessed towards tackling national security and defence issues, and to chart a course for progress amidst the declining security situation in the country under the auspices of the Defence Sector ICT Forum which is put up by Galaxy Backbone [1].

A. ICT: THE GOOD

Your ICT has been beneficial to National and Business Development in the following ways:

1) *Information And Communication*: Wide Communication gaps have been bridged with the advent of ICT through Mobile Communications and the robust connectivity it provides. Information can now be transmitted across geographical locations that are very far apart. This has ensured greater access to information, especially for formerly underserved populations. A 2008 report of the International Telecommunications Union (ITU) on the state of mobile and internet data in Africa revealed that Africa had 246 million mobile subscriptions and mobile penetration within the sub-region has risen from just five (5) percent in 2003 to well over thirty (30) percent within a span of five years.

Secure and Encrypted Mobile and Satellite Telephony Systems have also been produced for those who may want to transmit data securely, even though there are still altercations as to *"How legally permitted and morally acceptable within National Laws and Mores is the data being transmitted?"*

Hofstede, 2002, stated that "One of the most important features of the digital age is the use of new communications technologies to build digital citizenships. Cultures could be a source of conflict that affect the use of new media to make powerful collaborations among online communities across societies, and within the same society, however, there are still altercation between digital citizens, groups and nations."

Ibrahim Saleh also stated that "New [communication] media could help citizens in many directions such as appreciating their diversities; solving their problems, sharing experiences and voicing out their salient issues without worries and shame." Further observing that "the advent of ICT has brought about a new, global dimension to the operations of modern democracies and has, in effect, created a new "global public sphere," or a global civil society; this global public sphere, however, does not displace, but rather supplements national public spheres and governments."

Successes recorded in recent political campaigns across various parts of the world owe their mass mobilization to Short Messages, E-mails and Social Networking.

The INTELLIPEDIA was launched in 2006 by the United States Intelligence Community. It is a repository of information with varied degrees of classification and sensitivity for collaborative data sharing within the intelligence community and contains information on the regions, people, and issues of interest to the communities that use its host networks.

2) *Utilities*: ICT brings with it many utilities and capabilities that aid success and progress in various areas of world economy, such as: Education and Learning (using Computer Aided Instruction and Computer Assisted Learning), Construction and Manufacturing (using Computer Aided Design and Computer Aided Manufacturing), Banking and Industry (using Electronic Banking and Online Transaction Platforms), Advertising and Business Networking (using Computer Aided Advertising and Social Media), Health Care (using Computer Aided Diagnosis), to mention but a few.

3) Surveillance And Navigation: Using satellite and navigation systems, remote surveillance can be made across various geographically distant locations either for Security or Information purposes. Also, navigation could be carried out successfully through previously unknown locations using maps and positioning systems (such as the Global Positioning System – GPS), which are powered by ICT.

These systems could prove very useful in building Intelligence information and reports that could be very essential and invaluable in the task of thwarting and combating crimes.

4) *Security*: Former President Bill Clinton of the United States of America defined Critical Infrastructure as "those physical and cyber-based systems that are essential to the minimum operations of the economy and government." These systems include: Banking and Finance Systems, Electrical Power Systems, Emergency and Security Service Systems, Gas and Oil Production Systems, Storage and transportation Systems, Information and Communication Systems, Transportation Systems, Water Supply Systems, to mention but a few [7].

With Information and Communication Technology, the security of critical infrastructure has taken a new stride. Since the advent of Biometric and Chip-and-PIN hardware (cards) and tokens as methods of user authentication, critical infrastructure has been able to assume the very meaning of the name. Unauthorised access can hence be restricted based on a combination of various authentication methods.

5) *Shared Resources And Infrastructure*: Businesses and Government Parastatals are gradually emerging into an era where their operations, data processing, resources (hardware, applications) and infrastructure are managed and administered centrally and shared remotely amongst these various businesses and Parastatals who subscribe to these resources and services from end-user client equipment.

6) *Cloud Computing*: This is a cutting-edge facility provided by ICT in which data and information are stored remotely across very expensive and reliably safe server farms that span various data centres all over the world, and then made available to users in such a manner that is independent of geographical location, accessing device or connecting network. This has assumed a modern trend in ICT as it provides a cheaper means of deploying ICT Infrastructure, especially for businesses and organizations. Question and Concerns, however, still exist relating to the security and accessibility of information stored on Cloud Servers. These Clouds possess storage capacities that could be very awe-striking.

7) *Databases And Storage Consolidation Systems*: ICT provides sophisticated Database capabilities – which could be either locally administered or remotely managed – that could be implemented to store and centrally manage large volumes of sensitive and individual-specific information and deliver authenticated access to this information across various locations around the world using high-end Database Management Systems (DBMSs) that are super-reliable, very secure and capable of proactive remote back-up and recovery. Storage Consolidation is a capability of ICT that refers to the centralization, sharing and optimization of data storage resources among multiple users and application. It enables the design and construction of storage infrastructure for efficient management and maximum use, with the lowest possible storage hardware and management costs.

B. *ICT: THE BAD*

As ICT Infrastructure become more robust, diversified and advanced, the past decade has seen an exponential rise in Advanced Fee Fraud (popularly known as 419 Scams), Denial of Service (from critical infrastructure) Attacks and Social Engineering. Hack attacks have taken very dynamic trends as the Hackers have assumed very determined skills, all made easy by ICT. Also, other crimes that formerly had little to no Cyber Implications have become very popular / "lucrative" Cyber Crimes and Cyber-Fostered Crimes. Some examples that stare us in the face include: Prostitution (Adult and Child), Drug Trafficking, Child Trafficking, Child Pornography, Rape and other forms of Sexual Crimes, amongst others.

The recent advancements in Mobile Technology have made Mobile Devices a double-edged tool upon which National Security could leverage and with which it could also be breached. Information, some of which are unverifiable and false, is now placed within reach of the fingers of both those who understand them (or for whom the information is intended) and those who know absolutely nothing about the (usually very potent) information they have access to. The GSM Network, Short Messaging Service (SMS) (and E-mailing) have become very potent tools, even in the hands of the poor; and with the advent of Social Networking, the information dissemination boundaries are limitless [7].

Distance has ceased to be a barrier for criminals and subversives as ICT now provides the required infrastructure to communicate, network and strategize across geographically far-flung locations and execute the crimes remotely (from wherever they are on the globe). Reference [5] observed that be it the December 2009 bombing of the Superscreen TV station in Lagos; the terrorist-linked bombings in the Northern and other parts of Nigeria in recent years; the bombing of the Twin Towers of the World Trade Centre in 2001 in the U.S.; or the festering sectarian (and religious) violence in various parts of the world and the recent pervasive nature of armed banditry in our societies; these all owe their sophistication and devastation to the unrestrained and negative deployment of both cellular and other communication devices and the Internet [5].

Chats and Instant Messages (IMs), E-mails and the Short Messaging Service (SMS) have proved very potent over the past decade and Criminals have used them very useful in perpetrating various heinous crimes ranging from terrorism to armed banditry, laundering and rape. The SMS provides a means of remote, uncensored and unmonitored communication that is very cheap and accessible to both the rich and poor. Demonstrators have used it to mobilize protests, evade authorities, and spark off political spam, protests, riots and anti-government Campaigns in recent times. The Anti-Syria Protest in Beirut, Lebanon is a recent example. The protest mobilized over a million demonstrators through e-mails and text messages to demand the withdrawal of Syrian Troops from the Country and the resignation of Prime Minister Najib Mikati's government. In a similar report in 2008, 166 people were killed in a terrorist attack in Mumbai, India, which was believed to have been planned by extremists using mobile and satellite phones. A host of other historical Antecedents exist to further buttress and verify the potential of these services for Mass Mobilization, Mass Campaign and Mass Destruction.

Secure transmission of encrypted information – regardless of the nature of the information – became popular with the manufacture of the BlackBerry® – a line of wireless handheld devices and services designed and marketed by Research in Motion Limited (RIM) operating as BlackBerry®. Since the release of the first Blackberry® device in 1999, an e-mail pager, the device has faced chained prospects of being banned in Middle East Countries, the United Arab Emirates (UAE) and some Asian countries due to the nature of protected and strongly encrypted communications – which could not be monitored by the most National Governments and Agencies – that could be transmitted using the device; a potential propellant for terrorism and other illegal and nefarious activities. Despite claims that the RIM has managed to reach an agreement with the governments of such countries as Saudi Arabia and India in terms allowing some level of access to the information transmitted over the Blackberry® Network, these resolutions are only temporary at best; the reason being that the essential design of the Blackberry® devices prevents neither RIM, nor anyone else, from accessing the encrypted information transmitted on the Blackberry® Network. As at 2012, three million Blackberry® users were confirmed in Nigeria [16] out of the seventy-nine million confirmed global Blackberry® users and over 200 Million Blackberry® devices that have been shipped to date.

In recent years, the Research In Motion Limited has also risked bans from countries such as Indonesia and Singapore unless they could restrict the secure transmission of Pornographic Content using their Network as it violated the National and Moral Norms of the Countries and exposed them to Social Vices.

Displayed below is a Network Diagram of the Blackberry® Network:

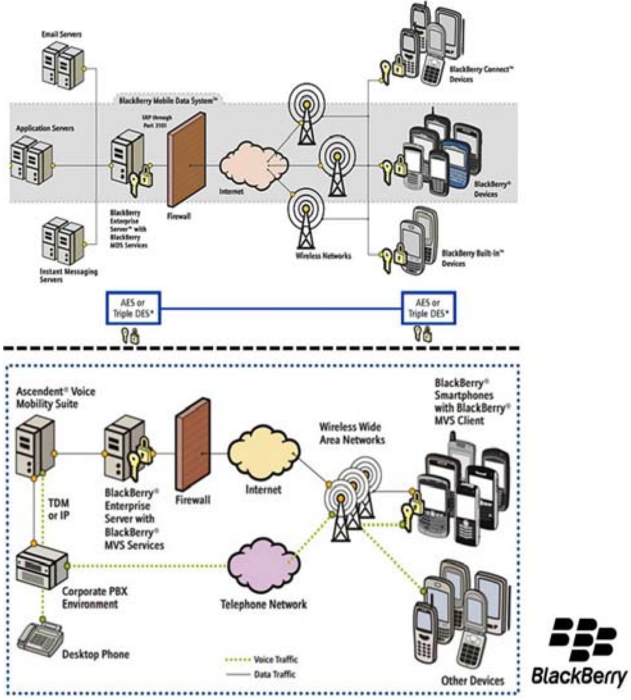
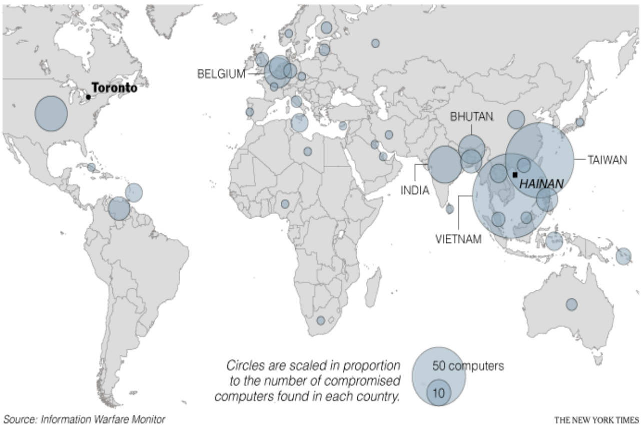

Email Servers
BlackBerry Mobile Data System™
SRP through Port 3101
Application Servers
BlackBerry Enterprise Server™ with BlackBerry MDS Services
Firewall
Internet
Wireless Networks
Instant Messaging Servers
BlackBerry Connect™ Devices
BlackBerry® Devices
BlackBerry Built-In™ Devices
AES or Triple DES*
AES or Triple DES*
Ascendent® Voice Mobility Suite
TDM or IP
BlackBerry® Enterprise Server with BlackBerry® MVS Services
Firewall
Internet
Wireless Wide Area Networks
BlackBerry® Smartphones with BlackBerry® MVS Client
Corporate PBX Environment
Telephone Network
Desktop Phone
Voice Traffic
Data Traffic
Other Devices
BlackBerry

Fig. 1 The Blackberry Network Diagram [18]

Remote Espionage has been made possible and relatively easy through the use of surveillance systems and utilities provided by ICT. In March 2009, researchers discovered a vast Chinese cyber-espionage network, codenamed GHOSTNET which was proven to have penetrated 103 countries, infecting at least a dozen new computers every week; so far, 1,295Compromised Computers have been discovered and were tracked to diplomatic and economic government offices of South and Southeast Asian Countries.

The network is designed to infiltrate sensitive ministries and embassies, one of the latest indications of China's determination to win a future "information war", having succeeded in majority of the cases. Further studies revealed that the GHOSTNET not only searches computers for information and taps their emails, but also turns them into giant listening devices. Once a computer has been infected, hackers can turn on its web camera and microphones and record any conversations within range [15].

The illustration below represents the vast reach of GHOSTNET as released by the New York Times Magazine, showing the locations of 347 of the compromised machines:


BELGIUM
Toronto
BHUTAN
TAIWAN
HAINAN
INDIA
VIETNAM
Circles are scaled in proportion to the number of compromised computers found in each country.
50 computers
10

Source: Information Warfare Monitor

THE NEW YORK TIMES

Figure 2: New York Times Report showing the locations of 347 of the Machines that have been compromised by GHOSTNET.

In a similar report in March 2013, the Herald Sun (an Australian daily) reported a Casino Scam in which a gambler used the casino's security cameras to spy for him as he played and made away with a whooping $32 million AUS (about $33.2 million) from Crown Casino in Melbourne, Australia – just some of the few and most recent discovered espionage cases [6].

The very same Mapping, Positioning and Geo-Navigation Systems that were invented initially to aid Navigators and Geographers in Navigating previously unknown locations have found another use in Navigating and Positioning Missiles, Warheads and Nuclear Weapons.

Gradually, the imminent is becoming more obvious as the initial “good” for which these ICT equipment and systems were invented to serve, gradually shifts from “bad” to “very ugly”.

C. *ICT: THE UGLY*

The growing trend is that these state-of-the-art ICT devices are gone beyond being the target of attacks, but have also become a covert means of launching them as well, unnoticed – a persisting fear that in the coming years, the deadliest of devices would become more within reach of the common citizen (both those who have legal intentions and those with nefarious motives) and at a very affordable price too; a garish situation that may deteriorate to a point where the disadvantages of the existence and possession of these ICT devices would begin to outweigh and effectively cancel out the advantages.

On January 12, 2012, a post emerged on a Portuguese blog [14] titled "A Declaration of the Independence of Cyberspace". The post essentially mocked the efforts of various National Governments to restrain the potentials of the Cyberspace, saying that "you (the national governments) have no moral right to rule (or control) us (the Cyberspace) nor do you possess any methods of enforcement we have true reason to fear", and further calling for freedom and independence for the Cyber-world and what can be inferred to mean a "Cyber-Nation". A reality which imminence we have good reason to dread.

Statements made by Dubai-based editor of the Middle East edition of Stuff magazine, Thomas Shambler made available on the website of world renowned television and news Channel – Al Jazeera – in 2010, revealed that, "Last year (2009), Etisalat [a national mobile-service provider in the UAE] sent out a text message to lots of its users," he says."That text message led users to download spyware. Days after the text message, which promised to improve service but actually contained eavesdropping software, was sent to UAE Blackberry® users, RIM issued a patch to remove the spyware, effectively thwarting the first attempt by the UAE Government to monitor Blackberry® communications in the Emirates."[17]

This put forth a reality that misgivings (by the manufacturers of ICT devices and ICT Service Providers) stemmed from a history of state-backed telecommunications surveillance in the region, which they viewed as breaches to the operations of their communications networks and the privacy of their clients – they obviously either could not see, or did not subscribe to the bigger picture; this poses a verifiable instance that creates some insight into a salient battle that puts on one side the Manufacturers of ICT equipment and devices trying to uphold the privacy of their clients and on the other side the National Governments trying to reclaim total control of their cyberspaces. The question now is, "*where do we stand?*"

III. THE PROBLEMS

A. CYBERSPACE

The Cyberspace is a virtual environment which exists not in the physical sense, but as a human-electronic community where people, systems powered by abstract concepts, and software interact. The Cyberspace exists upon an underlain electronic, network and communication infrastructure. Every country has its own cyberspace which is defined by the strength and capabilities of its National ICT Infrastructure. Even though the Cyberspace may appear borderless to users, it is limited by virtual borders which may appear seamless to the users; hence, Cyber-criminals perpetrate crimes in an environment they think is borderless.

Primarily, recent breaches and compromise in National Security using ICT can be traced and linked directly to unmonitored, poorly administered and unrestricted National Cyberspaces. In underdeveloped and developing countries, the concept of a Cyberspace is perceived as an abstract, unrealistic phenomenon crafted possibly to rapidly deplete both foreign and local national reserves. This has resulted in a gross neglect of these cyberspaces which have now formed a haven for Cyber Subversives and Criminals; the Cyberspace has become a lawless zone where transmissions and communications that explicitly violate constitutional provisions and threaten peace and security are carried out with wanton abandonment.

A 2008 report of Cyber Crimes Complaints from the Internet Crime Complaint Centre (IC3) – a body setup to investigate internet crimes – revealed that Nigeria is ranked Number Three (3) in the list of countries that have been mostly associated with Reported Cyber Crime Cases. The statistics are shown in the Figure below:

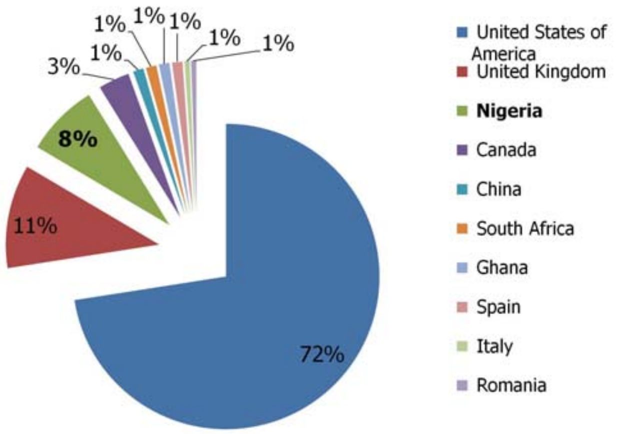


Figure 3: 2008 Report of the Internet Crime Complaint Centre showing countries with the highest numbers of Internet Crime related complaints [7]

Sadly, the mobile telecommunications giants who champion the cause of intelligence surveillance and the monitoring of Cyberspace transmissions in developing countries have been so helplessly and hopelessly hypnotized by the prospects of profit making in developing and underdeveloped countries that they have failed to realize that the absence of National Peace and Security pose a very potent threat to their business existence and operation within the geographical borders of the Nation; a fact that has been further emphasized by the recent bombings and arson to telecommunications facilities and stations as well as the killing and maiming of telecoms staff in various Northern Nigeria States.

However, we wish to commend at this point the laudable efforts of the Nigerian Communications Commission (NCC) being geared towards regularizing the mobile telephony and telecommunications industry in Nigeria for a better centralized management and efficient administration through the recently concluded SIM (Subscriber Identity Module) Registration and on-going SIM Verification processes and also by the drafting of the Lawful Interception of Communications Regulations.

The lack of adequate, comprehensive record keeping in underdeveloped and developing countries is poses another inherent problem; a problem which sadly has also plagued quite a number of "developed" countries to a verifiable extent. Many developing countries cannot lay a precise hold on the number of individuals in its citizenry; hence, a lot of these are based on approximations. Two separate approximations of the Nigerian Population by the United Nations and the Nigerian Population Commission put the citizenry at 162.5 million and 162,471,000 in July 2011 while the Population of the United States of America was put exactly at 312,780,968; Switzerland at exactly 7,954,700 and Canada at 34,482,779 after a population census that was conducted at about the same period. This inability to provide precise, accurate and pedantic count statistics of the citizenry further highlights this problem. This problem has made the task of monitoring and tracing extremely difficult and unverifiable in developing and underdeveloped countries and made it more impossible government to account for citizens at any given time.

Another problem is the fact that ICT Infrastructure and Systems are deployed in most countries without adequate provisions for the internal security of these infrastructure systems at the design and implementation stages of the deployment of these infrastructures. These Systems are deployed with numerous exploitable vulnerabilities inherent in their very design and fabrication.

Security usually comes as an after-thought for the most part, if the need for it ever arises at all. In 2011, the International Standards Organization (ISO) published the document: ***ISO/IEC 27031:2011***. This Document describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to that identify and specify all aspects (including performance criteria, design, and implementation) for enhancing an organization's ICT readiness to ensure business continuity.

These specifications apply to any organization (private, governmental, and non-governmental, irrespective of the size) that is concerned with developing its ICT readiness for business continuity (IRBC), and require its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions; enabling an organization to measure performance parameters that correlate to its IRBC in a consistent and widely recognized manner. A summary of the process cycle is shown in the figure below:

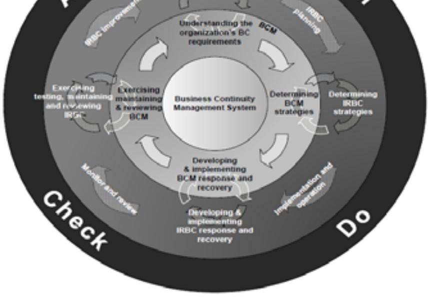

Act
Plan
Check
Do
Understanding IRBC requirements
IRBC
IRBC planning
IRBC improvement
Understanding the organization's BC requirements
BCM
Exercising testing, maintaining and reviewing IRBC
Exercising maintaining & reviewing BCM
Business Continuity Management System
Determining BCM strategies
Determining IRBC strategies
Developing & implementing BCM response and recovery
Monitor and review
Implementation and operation
Developing & implementing IRBC response and recovery

Figure 4: Figure illustrating the Integration of ICT Readiness for Business Continuity (IRBC) and Business Continuity Management System (BCMS) [11]

However, the extent to which this standard has been adopted by organizations and national governments still remains grossly unverifiable for the most part.

IV. Possible Solutions

On September 29, 2000, the Independent Corrupt Practices Commission (ICPC) was formed in Nigeria and empowered by the Corrupt Practices Act, 2000 to investigate corruption and prosecute criminals in line with the codes prescribed by the Act [12]. In 2003, a similar body was formed – the Economic and Financial Crimes Commission (EFCC) – in Nigeria and empowered by the Economic and Financial Crimes Commission Establishment Act of 2004. The Commission is empowered by the Act to prevent, investigate, prosecute and penalise economic and financial crimes (such as the advance fee fraud and money laundering in concertion with the efforts of the international community in fighting money laundering) and is charged with the responsibility of enforcing the provisions of other laws and regulations relating to economic and financial crimes, including: The Money Laundering Act 1995, The Money Laundering (Prohibition) act 2004, The Advance Fee Fraud and Other Fraud Related Offences Act 1995, The Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, The Banks and other Financial Institutions Act 1991 and Miscellaneous Offences Act [13].

The ICPC and the EFCC remain the closest the government of Nigeria has come to efficient Cyber Law Enforcement and Criminal Prosecution, but they still stand deficient in the task of meeting the big picture of Cyber Security.

These Commissions have however fulfilled their mandate within the verifiable limits of why they were established; but still, they remain not enough. This is largely because they function outside of the Cyberspace environment. They are positioned – by reason of the constraints of their mandate and the lack of adequate Monitoring and Surveillance Infrastructure – outside the borders of the Cyberspace and hence, have limited contact (and influence), if any at all, with (and on) the activities that take place within the National Cyberspace.

This spate can be representative of the condition that has plagued most developing and underdeveloped countries to date, subject to verification.

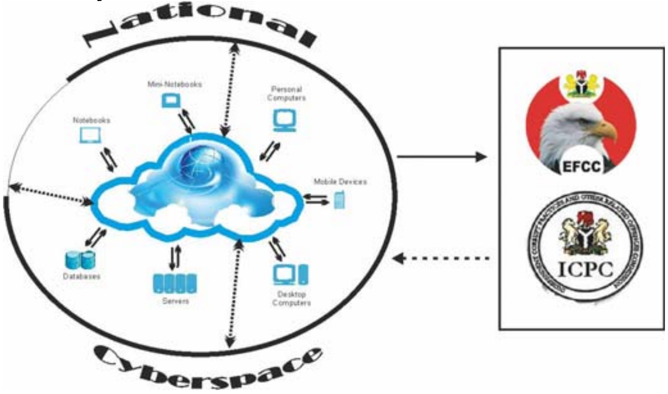


Figure 5: Figure illustrating the degree of interactions and relations between the EFCC and the ICPC of Nigeria and the National Cyberspace: "WHAT WE HAVE"

Their operations are mainly reactive in nature; reacting to reported cases of financial crimes, cyber crimes and corruption.

We must at this point emphasize the verifiable fact that a greater percentage of the National Security Challenges faced by most developing and underdeveloped countries can be linked directly or indirectly, in more ways than one to the problem of poorly guarded or completely unguarded Cyberspaces. This necessitates the need for proactive law enforcement and policing within the boundaries of every National Cyberspace. **EVERY** transmission that goes in, within and out must be verified, validated and authenticated as legal and constitutionally allowable within the laws of the Nation and the International Community. Short Messages, Calls, Faxes, E-mails, and all other means of data and information transmission and communication must be monitored and verified (having a known and verifiable origin and destination) in real time, at all times. Suspicious transmissions should then be quarantined and monitored more closely or blocked out rightly.

Following the 9/11 attack on the Twin Towers in the United States, an attack the country attributes to a failure in intelligence on their part, America and other European Countries that have suffered similar attacks have proven inexpugnable by such crimes ever again to verifiable extents as appropriate technology and infrastructure were deployed immediately to keep tabs on and gather intelligence from every transmission (cellular and internet traffic) that went in and out of their Cyberspace, especially transmissions that involved such keywords as *Allah*, *Al-Qaeda*, *Bomb*, *Invade*, *Attack*, to mention but a few.

Similar measures must be adopted by developing and underdeveloped countries if the spate of national insecurity is to be alleviated; ICT Systems should be fitted with sophisticated intelligence gathering and monitoring facilities that would help to forestall crimes, expose those that are on-going and propel investigations of the few that would manage to escape surveillance.

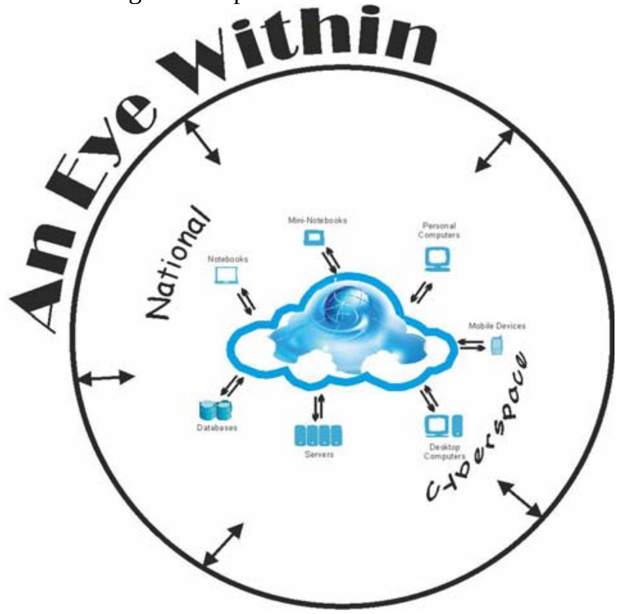


Figure 6: Figure illustrating monitoring of transmissions and communications within National Cyberspaces: “WHAT WE NEED” – An Eye Within

Every Nation must come to terms with the fact that her Cyberspace is her sole responsibility and she must guard it with every facility and resource at her disposal or put her National Security on the line. It may be impossible or difficult for a Government to monitor standalone computers it does not own, but an obvious truism is that if a nation assumes total responsibility for her Cyberspace, then whoever is transmitting information would be bound to abide by the rules or risk disconnection and / or prosecution.

ICT provides Infrastructural capabilities for keeping comprehensive citizenship records of every citizen of the country with utmost accuracy and precision. The records could be duly collected at critical points such as birth places, points of health care delivery and other such locations, and stored across very potent and capable databases which can be managed and accessed from a centralized location. This would ensure that every citizen of the Nation can be accounted for by its Government at any point in time; thus, greatly simplifying the task of monitoring and tracing as comprehensive specific records of the individuals in the citizen population (down to the Biometrics) can now be accessed by the click of a button.

Regulations and Legislations should be put in place for the enforcement of proven and tested standards such as the ***ISO/IEC 27031:2011*** standard in developing and underdeveloped countries. This would help guarantee that ICT Infrastructure and Systems that have been deployed in any country adhere to proven world standards and hence would pose minimal to no threat to the Nations’ Cyberspace.

Intelligence Reports should remain classified and made available only to licensed members of the National and International Intelligence Communities or other authorized individuals. Transmission of such classified reports must be done securely and over covert transmission channels in order to prevent them from falling into the wrong hands. The growing sophistication in security challenges especially the trans-national nature of most, and the advances in technology, have more than ever before underscored the importance of a multi-sectoral, holistic and integral approach in intelligence management.

ICT Security and Usage policies should be established at all levels of government, Parastatals and organizations, especially in developing and underdeveloped countries, in order to govern and more clearly define and determine what is allowable and what is considered as a breach to national security or a threat to business progress, and this policies should be made known and enforced on all business and organizational (governmental or non-governmental) networks within the country.

Concertedly, also, [8] opined that “ICT could be a path towards peace, security by embracing the principles of participatory governance on the one hand, and implementing them through user friendly harmonized, effective and efficient management tools and mechanisms on the other. The latter and more specifically those responsive to the populations needs in harmony with the environment will enable governments to better channel development actions in order to obtain a positive and sustainable impact and address the challenges faced by African countries.” [8]

V. CONCLUSIONS

We have come to a point in human history where the task of national security transcends the strength (in terms of numbers) of the Armed Forces, the sophistication of their weapons arsenal and the brilliance of their battle and defence strategies and tactics; technology provides speed, robustness, sophistication, potential and capacities that outwit all these.

"The Nigerian public expects much from us (law enforcement agents) and as the saying goes: to whom much is given, much is expected. (Imagine) An occasion where we are fighting almost bare-handed and given the strong political, economic, social, cultural and other problems, that make policing so frustrating in our country; we can only still give our best. And I say to all officers who have had to lay down their lives in the line of duty, may God accept your souls in perfect peace. Amen. May your sacrifices not be in vain." – Former IGP, Mr. Ogbonnaya Onovo (Nigerian Compass, 14th September 2010)

Wars are being initiated, fought and won daily in Cyberspace with every spam e-mail that passes unnoticed; every text message or call that is transmitted without being monitored and every connection that is initiated in Cyberspace without being verified and properly authenticated.

"The current security situation in the country (Nigeria), to say the least, is condemnable and unacceptable to the government and good citizens of our great nation. I therefore believe that the time has come for the Nigeria Police High Command to review its strategies in order to perform its duty. No responsible government would fold its arms and watch helplessly as its citizens are being maimed or cut down in their prime when there is a police force in place." – Dr. Ibrahim Lame, former Minister of Police Affairs (The Punch, 5th March 2010).

What is obvious (as even from the statements quoted above) is that, like in some other parts of the world, the crime rate is gradually overwhelming the national security outfit in terms of personnel, machinery and tactics. The ever-widening gap between our national security budgets and the rising tide of crime calls for a spontaneous deployment of scarce resources in the war against crime. Responses to crime problems should be more proactive with the use of security intelligence to locate people and activities that are suspected to pose (future) threats to national peace, rather than simply reacting to reported crime cases. The former is sure to result in more budgetary savings coupled with the benefits of proactive maintenance of law and order.

Nobel Laureate, Prof. Wole Soyinka, in a May 8, 2013 video conference interview with privately owned television station, Al Jazeera, described the state of the nation (Nigeria) as a war situation judging from the incessant killings of innocent people by the terrorist Islamic sect, Boko Haram; stressing that the phenomenon should not be regarded as being limited to the Northern region alone or Borno and Yobe states, but it should be seen as affecting the entire country. He further decried the way and manner the Federal Government was handling the insurgency; saying it was looking at it as a short-term phenomenon that could be tackled with short-term solutions.

On the part of our African Governments, Ibrahim Saleh observed that "Emerging experiences in the world show that the ICT achievements that leave lasting impacts require visionary leadership with sound management systems and tools in place to enable the translation of principles into concrete actions that would generate expected results in the end. Thus requiring a coalition of the attributes of being well-trained with the skills and vision needed to provide a new niche of public sphere where views about standards can be aggregated; leading to the creation of an enlightened citizenry that is reflective of social mixes within our individual societies."

We would say that for National Security to be restored, our Nations and Government must rise to their responsibilities and take back control of their Cyberspaces and the transmissions that go on therein, before they are completely lost to resolute subversives. As the user-base keeps evolving, and more sophisticated devices keep emerging, it becomes only imperative and inductive that the National Security forces dynamize proactively in order to manage the new trend of events. Furthermore, we would also emphasize the fact that the responsibility of National Security lies also in the hands of the citizenry and not the government alone. Every suspicious transmission, communication (electronic or oral) within the circle of reach of every citizen must be reported to the appropriate authorities for prompt action to be taken; National Security is all about people, and the people must duly contribute their quota as we all strive to restore Peace and Security to our Nations.

ACKNOWLEDGMENT

We would like to acknowledge the efforts put in by the Managements of Babcock University and University of Jos, in providing a conducive environment and adequate infrastructure for us to be able to conveniently carry out the necessary research required in producing this paper.

REFERENCES

[1] Everest Amaefule (May 3, 2012); Stakeholders to explore ICT Role in National Security – The Punch Newspaper [Online]. Available: http://www.punchng.com/business/close-up-on-ict/stakeholders-to-explore-ict-role-in-national-security/

[2] (2012) Sophos Website [Online]. Available: http://nakedsecurity.sophos.com/2012/10/19/data-leak-google-stock/

[3] http://searchcio-midmarket.techtarget.com/definition/ICT

[4] ICT Security Services End-to-End Solutions (2013) [Online]. Available: http://www.t-systems.com/solutions/end-to-end-security-for-ict-systems-t-systems/759956]

[5] J. Uwaya, "Our National Security and the Raging ICT Revolution" (2011) [Online] Available: http://nigeriavillagesquare.com/articles/guest-articles/our-national-security-and-the-raging-ict-revolution.html]

[6] (2013) Huffingpost Website [Online]. Available: http://www.huffingtonpost.com/2013/03/15/crown-casino-scam-32-million-australia-_n_2884933.html

[7] A. Ajijola, "The role of ICT Deployment for National Security," in ENIGERIA 2010 Conference,.

[8] I. Saleh, "The impact of ICT on Peace, Security & Governance in Africa," University of Cape Town, Centre for Film and Media Studies. [Online].

Available: http://www.academia.edu/393239/The_impact_of_ICT_on_Peace_Security_and_Governance_in_Africa

[9] Google Search [Online]. Available: http://www.google.com.ng

[10] WIKIPEDIA website. [Online]. Available: http://en.wikipedia.org

[11] International Standards Organization Website. [Online]. Available: http://www.iso.org

[12] Independent Corrupt Practices Commission (ICPC) Website [Online]. Available: http://icpc.gov.ng/legislative-background/

[13] Economic and Financial Crimes Commission Website [Online]. Available: http://www.efccnigeria.org/efcc/index.php/about-efcc/the-establishment-act

[14] [http://dieelektrischenvorspiele.wordpress.com/2012/01/18/a-declaration-of-the-independence-of-cyberspace/]

[15] http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html

[16] Heydary Hamilton PC Lawyers. Inside the RIM: Decrypting the Blackberry. Newsletter Publications. Canadian Lawyers, Patent & Trade-Mark Agents. (2013)

[17] Al Jazeera News. Behind the Blackberry Ban. [Online]. Available: http://www.aljazeera.com/focus/2010/08/20108516113706244.html

[18] BlackBerry Mobile Voice System (MVS) Part II: Understanding How BlackBerry MVS Works [Online]. Available: http://www.blackberry.com/newsletters/connection/it/i608/understanding-mvs.shtml