Evaluating the Security of E-government in West Africa

By

Oyesola Oke
Lewis University

May 6, 2009

Abstract

The Internet and technological advances has reshaped the global business in government and industry throughout the world. African governments have realized the need to develop an information and communication technology infrastructure to improve their current and future development. Hence, there is rapid growth of e-government in West African countries, geared at improving efficiency and effectiveness of government. The use of Internet has increased for the past ten years to ease access to information. People use Internet to transact business, to email, to pay bills and apply for jobs. Also usage has grown, so too, has the risk of vulnerability. Information is accessed by different kinds of people with different levels of access and this often leads to information security issues and eventually lead to information security being compromised. Thus, government must maintain effective mechanisms and security controls when sensitive data belonging to citizens is concerned. Systems must be designed to guarantee compliance with existing privacy and data security regulations, policies and standards.

The purpose of the paper is to evaluate e-government security practices in West African countries in the context of electronic government applications. The main discussion will be on the e-government security policy issues, security control, and regulatory compliance, emerging techniques, access issues and e-government readiness.

TABLE OF CONTENTS

Introduction

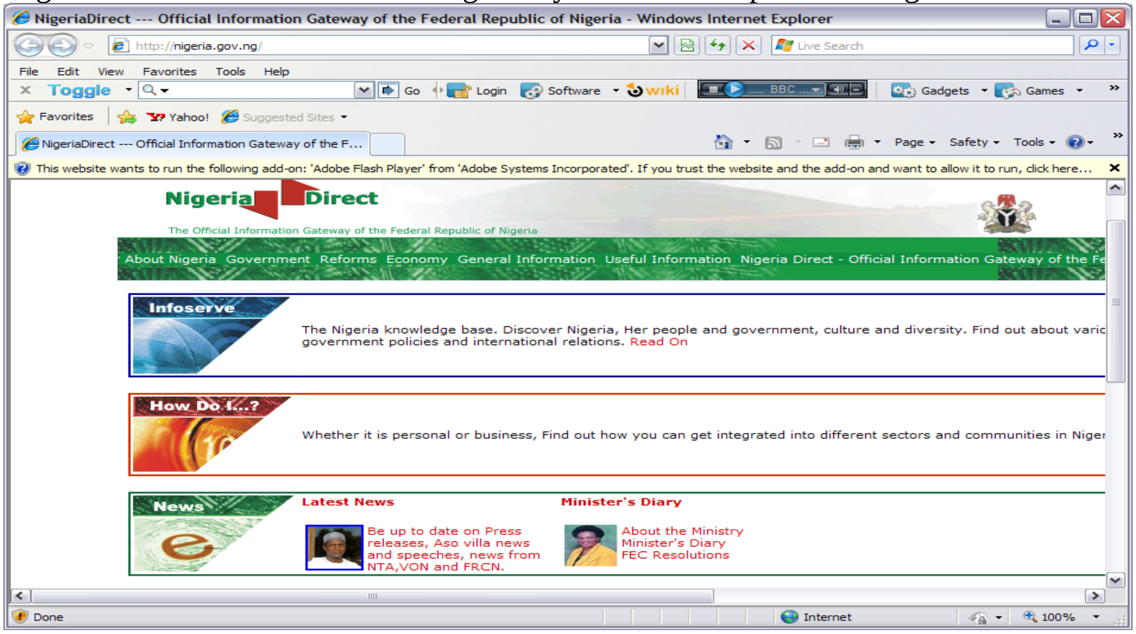
The Internet along with modern technological advancement has changed the way the government and industry do business through the West African region. It creates quick and more efficient ways to do business, but the reality of increased economic crime having a serious impact on the global economy. According to data available currently, it estimates that the global economy loses more than $200 billion dollars annually, in direct and related damages from Internet crime, which threatens global stability and security. But the effect of the growing challenge of Internet crime, to developing economies translates into a complete digital nightmare. Nevertheless, West Africa has come a long way from the Non-existent stage, to initial, to an intuitive stage, in implementing e-government, e-commerce initiatives and eletronic banking.

The demand for e-banking is increasing at an exponential rate, in response to a public will to reduce the number of in-person cash transactons. With the increase in the rate of armed robberies, it is unsafe to perform usual business transfers with cash. Hence, communities are demanding the more secure electronic banking, for faster connectivity to facilitate smoother business operations. The banks that are slow in implementing the e-banking are losing customers to their competitors who have invested in the reform to electronic transfer.

There is no unity in e-banking in West Africa. Some banks use mobile-bank which is mainly mobile banking transaction, and some use x-bank which means cash card exchange managed by each banks. Many African banks have learned the painful processes involved in Wireless Application Protocol (WAP) Banking. The Offshore transfers of WAP banking technology was a disaster for the business community seeking reform and security with banking. It was an internet-based technology that relied on mobile phone usage, resulting in an experience that was slow, unreliable and costly for consumers in a continent with expensive mobile internet cost, poor coverage, hand set limitations and inadequate customer education.
Many African countries involved in this reform are at the Initial stages of E-government only South Africa has progressed to the Defined stage of E-government. South Africa's overall security policy is defined and follows a structured approach, and her security awareness protocol is communicated with all its citizens. Nigeria and Ghana are in the Intutive stage of E-government. There are no inconsistencies with the overall security policies. The security risk is managed on an as-needed basis. The security risk decisions are recognised in an intuitive way. Recently, Nigeria introduced the E-service into policy discussions concerning E-government.The E-Services applications was designed for the delivery of information or services to citizens. The desirable features of these applications are the organization of information according to customer profile, the capability to allow a customizable experience, and the ability for the user to achieve transparency with the agency and their government. The government portal aims at one-stop-shopping to provide comprehensive information and to deliver integrated government services. The government portal is divided into four sub-portals; (see figure 1 and 2 below) the web sub-portal offers a gateway

of information for citizens, small businesses and other government agencies. The Citizen sub-portal provides useful information and services to the citizens, including e-services such as applications for Driving License, Income Tax, business registration, government job vacancies and Passport & Immigration. Applicants are required to register to use these e-services.

NigeriaDirect. Official information gateway to Federal Republic of Nigeria.


NigeriaDirect --- Official Information Gateway of the Federal Republic of Nigeria - Windows Internet Explorer
http://nigeria.gov.ng/
Live Search
File
Edit
View
Favorites
Tools
Help
Toggle
Go
Login
Software
wiki
BBC
Gadgets
Games
Favorites
Yahoo!
Suggested Sites
NigeriaDirect --- Official Information Gateway of the F...
Page
Safety
Tools
Done
Internet
100%

This website wants to run the following add-on: 'Adobe Flash Player' from 'Adobe Systems Incorporated'. If you trust the website and the add-on and want to allow it to run, click here...

Nigeria Direct

The Official Information Gateway of the Federal Republic of Nigeria

About Nigeria Government Reforms Economy General Information Useful Information Nigeria Direct - Official Information Gateway of the Fe

Infoserve

The Nigeria knowledge base. Discover Nigeria, Her people and government, culture and diversity. Find out about varic government policies and international relations. Read On

How Do I...?

Whether it is personal or business, Find out how you can get integrated into different sectors and communities in Niger

News

Latest News

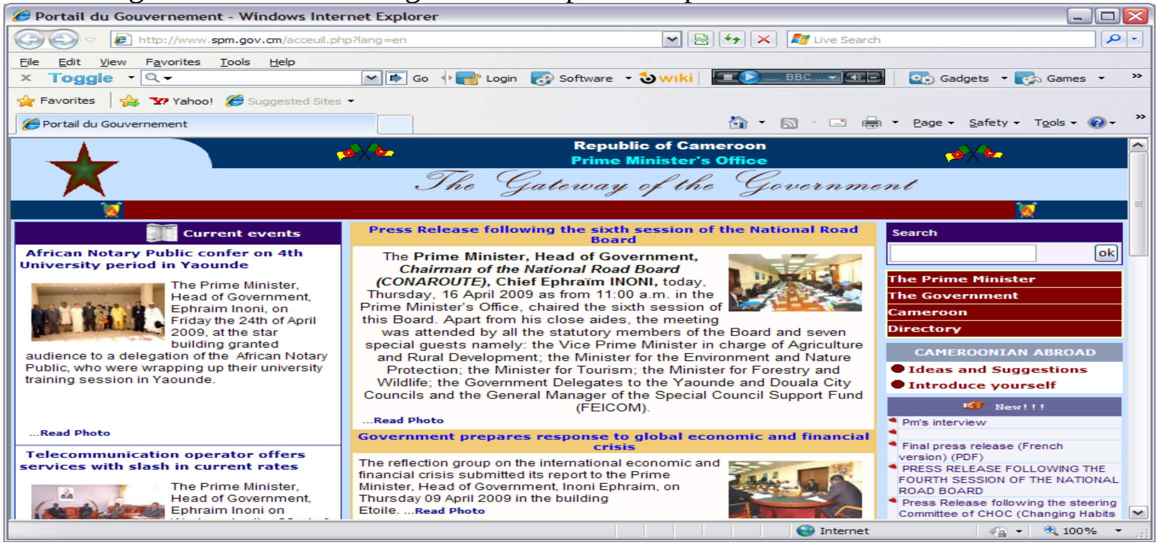
Be up to date on Press releases, Aso villa news and speeches, news from NTA,VON and FRCN.

Minister's Diary

About the Ministry
Minister's Diary
FEC Resolutions

Figure 1.

Portal du government. Official government portal Republic of Cameroon.



Republic of Cameroon
Prime Minister's Office

The Gateway of the Government

Current events

African Notary Public confer on 4th University period in Yaounde

The Prime Minister, Head of Government, Ephraim Inoni, on Friday the 24th of April 2009, at the star building granted audience to a delegation of the African Notary Public, who were wrapping up their university training session in Yaounde.

...Read Photo

Telecommunication operator offers services with slash in current rates

The Prime Minister, Head of Government, Ephraim Inoni on

Press Release following the sixth session of the National Road Board

The **Prime Minister, Head of Government,** ***Chairman of the National Road Board (CONAROUTE)*****, Chief Ephraïm INONI,** today, Thursday, 16 April 2009 as from 11:00 a.m. in the Prime Minister's Office, chaired the sixth session of this Board. Apart from his close aides, the meeting was attended by all the statutory members of the Board and seven special guests namely: the Vice Prime Minister in charge of Agriculture and Rural Development; the Minister for the Environment and Nature Protection; the Minister for Tourism; the Minister for Forestry and Wildlife; the Government Delegates to the Yaounde and Douala City Councils and the General Manager of the Special Council Support Fund (FEICOM).

...Read Photo

Government prepares response to global economic and financial crisis

The reflection group on the international economic and financial crisis submitted its report to the Prime Minister, Head of Government, Inoni Ephraim, on Thursday 09 April 2009 in the building Etoile. ...Read Photo

Search

ok

The Prime Minister
The Government
Cameroon
Directory

CAMEROONIAN ABROAD

- Ideas and Suggestions
- Introduce yourself

New! ! !

- Pm's interview
- Final press release (French version) (PDF)
- PRESS RELEASE FOLLOWING THE FOURTH SESSION OF THE NATIONAL ROAD BOARD
- Press Release following the steering Committee of CHOC (Changing Habits

Figure 2.

The Government sub-portal offers secured online services and information for Government employees. It also offers online information to improve inter-governmental collaboration, which includes resources for civil servants (conditions of service, job vacancies and governmental structure), code of ethics for public servants to promote effective administration and the guidelines for responsible behavior. The Non-Citizen sub-portal is a web-based platform allowing interactions between non-citizens and the government. It provides information to foreign citizens, tourists and foreign investors and information about the country. The Business sub-portal provides detailed information to the business community, with the aim of reducing administrative procedures hence increases government's efficiency. It stimulates entrepreneurship, investments and overall reduces the corruption within the government empire.

What is e-government?

E-government is online government or Internet-based government that use electronic technologies to exchange information and services with citizens, businesses, and other arms of government. E-government may be applied by the legislature, judiciary, or administration, in order to improve internal efficiency and the delivery of public services. In advanced countries such as the United States, government has variety of services for the citizen such as online bill payment, online change of address, online stamp purchase, online job application and online tax filing. Also, in United Kingdom such service is available for citizens and the businesses.

There are many benefits from e-government (Zhiyuan Fang 2002[1] this includes better and more profitable engagement with citizens, higher productivity, more efficient administrative procedures, the strengthening and growth of democracy and finally, the provision of high quality online services as well as improvement of the existing ones·

Information Security Policy Issues

The world of Internet is faced with security and privacy issues, and with growing popularity of e-government in West Africa, the governments and the citizens are now beginning to raise issues related to Internet security and privacy (Heeks, Richard 2002)[3]**.** In Western world, there is a sound legislative and policy regime that deals with the Internet security and privacy issues. In United State for example, there are laws enacted that govern Computer Misuse, Computer Privacy, Electronic Transactions, Computer Crimes, Computer Security Enhancement, Data Retention Laws, Digital Signatures and Computer Evidence Laws have enacted to punish the offenders. Also, not long ago the G8 24/7 Network had a Convention on cyber crime that was designed and signed into law.

The provision of the Convention on cyber crime is call Article 35[9], that is, the creation of points of contact that must be available 24 hours a day, 7 days a week, to facilitate international cooperation. The parties to the Convention are thus to establish such 24/7 contact points and this legislation affects all offenders worldwide. Council of Europe action against cyber crime Article 35 – 24/7 Network, "Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures”.

The success of E-government in Africa depends on the security of the data and other infrastructures. Some of the long-standing needs and concerns of the region have been privacy, confidentiality, and security of government information. Since information technology has been proven beyond doubt as enabling path to Economic development, West African governments must diligently emplace appropriate policy and legislative regimes to effectively govern E-government development.

There is an urgent need to balance privacy and access issues, and to develop guiding principles, policies, and legislation to ensure that the most valuable information to the public is protected with underlying due-diligence. Unfortunately, many African countries, Nigeria in particular does not have any reliable law to deal with internet crime, though she represents the largest single concentration of people of African descent in the world, and is also the 6th largest oil producer in the world as well as the 7th most populated nation on this planet. If any attack should happen to e-government infrastructure, this could be disastrous and consequently paralyze the machinery of government.

In South Africa, government and banking sector takes cybercrime seriously by enacting legislation that substantial and procedural laws that criminalize certain activities online. The Act also creates procedures for investigation, prosecution, punishment and sentencing of offenders, while enhancing global collaboration in cybercrime and cyber security enforcements.

With the use of information technology on the rise, access to sensitive and personal information has been easy for more cyber criminals and hackers, which creates new security risks. There are potential risks associated with use of electronic systems to access information and sharing of sensitive information online. Since it is necessary for information to be accessed by government employees to do their day-to-day duties, by private agencies and by public, hence the sensitive information is exposed to various levels of people including the hackers and cyber criminals. Therefore, many aspects have to be considered in regards to such online availability of information, for example, training people how to access and protect information, ensuring adequate levels of security, confronting ethical issues and maintaining the availability of information at crucial times. It is paramount that all the role players in e-government be educated about the vitality of security and train their employees on the value they placed on privacy of its information as well implementation of the privacy protection.

There many security frameworks that are available throughout the globe, this includes: COBIT, ISO 17799 and NIST that can be adopted by African government.

COBIT

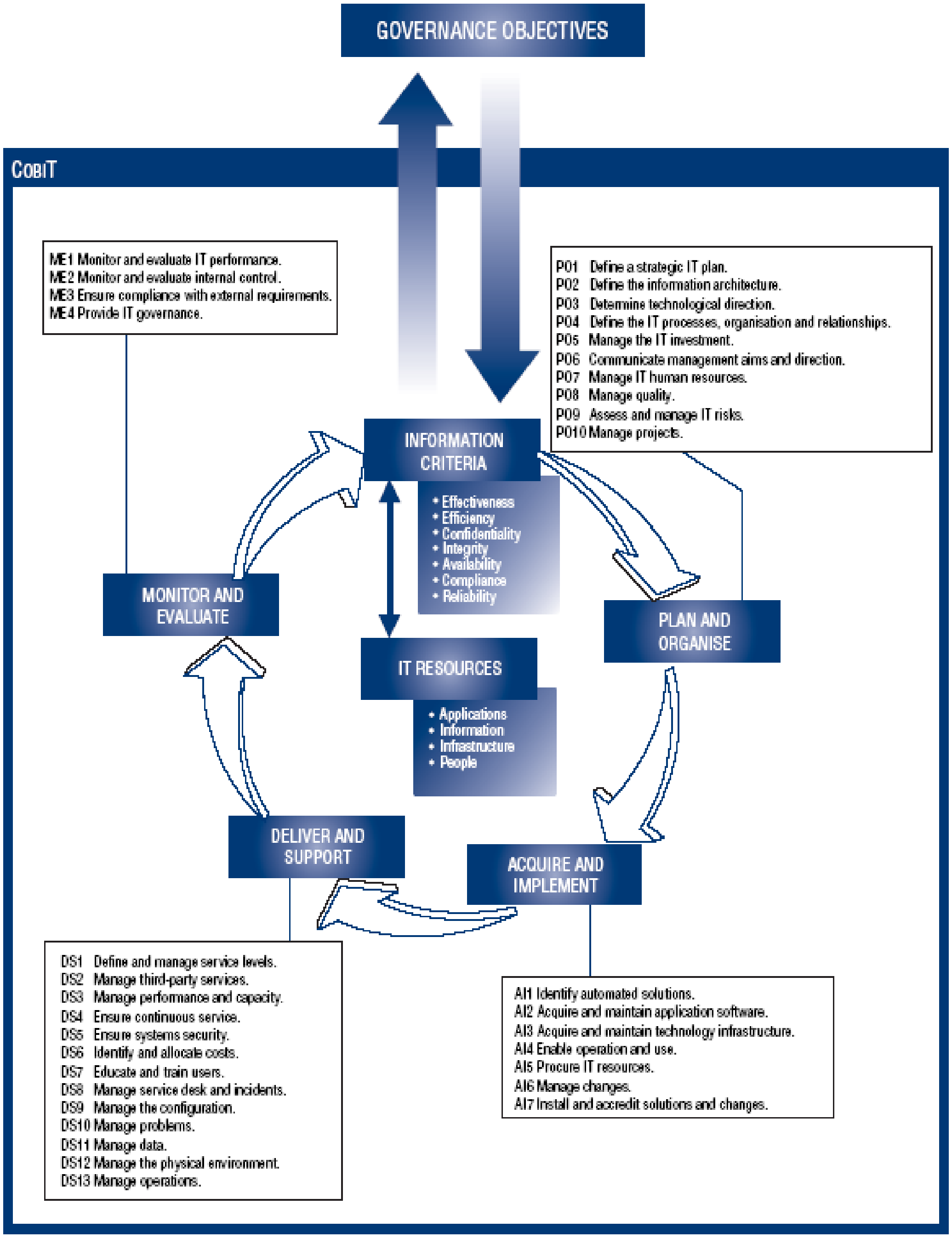
The Control Objectives for Information and related Technology (COBIT) framework can be use for best practices in Africa as a baseline for information technology (IT) management controls. It is used as security framework all over the world. It is created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992. COBIT provides managers, auditors, and IT users with a set of generally accepted measures indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework. If African governments could adopt the COBIT framework, it will help them to bridge the gap between control requirements, technical issues and business risks.

COBIT has 34 IT processes that are grouped into four domains.

The four domains are: (see figure3).

- Plan and Organise which provides direction to solution delivery and service delivery.
- Acquire and Implement provides the solutions and passes them to be turned into services.
- Deliver and Support - receives the solutions and makes them usable for end users.
- Monitor and Evaluate - monitors all processes to ensure that the direction provided is followed.


GOVERNANCE OBJECTIVES
COBIT
ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.
PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.
INFORMATION CRITERIA
• Effectiveness
• Efficiency
• Confidentiality
• Integrity
• Availability
• Compliance
• Reliability
MONITOR AND EVALUATE
PLAN AND ORGANISE
IT RESOURCES
• Applications
• Information
• Infrastructure
• People
DELIVER AND SUPPORT
ACQUIRE AND IMPLEMENT
DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.
AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

IT GOVERNANCE INSTITUTE

Figure 3. Shows various elements of COBIT framework

ISO 17799 and NIST

Another widely used standard in African countries is National Institute of Standards and Technology (NIST) and International Standards Organization (ISO). ISO 17799 Framework of Security is being widely used in Africa especially by Nigeria, the most part of ISO standards and the NIST standards that are widely use is the management of information security that requires the following:

- *Asset Identification and Assessment:* Identify the information and physical assets that must be protected within an organization
- *Risk Assessment and Analysis:* Conduct an assessment of the risks and analyze them against the probability of occurrence
- *Implementation of Safeguards to Counter Identified Risks:* For risks that are identified as having a high probability of occurring, implement reasonable and appropriate safeguards to lower the probability to an acceptable level
- *Addressing Third-Party Security through Contracts or Service Provider Agreements:* Control potential risks created by third parties through the use of contracts that require third parties to implement reasonable and appropriate safeguards when they process, store, use, or transmit organizational assets
- *Training:* Train Employees, Teachers, students, and citizens on policies and procedures and other safeguards and security practices to protect organizational assets.
- *Monitoring and Testing:* Regularly monitor and test the effectiveness of implemented safeguards against known or potential risks.

Payment Card Industry Data Security Standard (PCIDSS)

Since the inception of Visa and Master card in West Africa, PCIDSS standard has been adopted and implemented throughout the region. Payment Card Industry Data Security Standard (PCIDSS) is a security standard requirement for security management, policies, procedures, network architecture, software design and other critical protective measures. Any business or government that uses Visa or Master Card must comply with their regulations.

The Computer Misuse Act (1990) The 1990 Computer Misuse Act Chapter 18 section1 was introduced by Parliament to prevent misuse of computers[9]. The effect of the Computer Misuse Act was to make it a criminal offense to gain access to a computer without permission. The Act was also based upon the recommendation of the UK Law Commission, which at the time saw the need to address the increasing number of instances in which computer networks were being hacked by third parties, and also to recognize the international nature of such offenses.

Under Section 1 of the Act, a person is guilty of an offense if:

- he causes a computer to perform any function with an intent to secure access to any program or data held in the computer;
- the access he intends to secure is unauthorized; or

- he knows at the time when he causes the computer to perform the function that this is the case.

Section 3 of the Act addresses the unauthorized modification of computer material. Under this provision, a person is guilty of an offense if he does any act, which causes an unauthorized modification of the contents of a computer, and at the time when he does the act he has the requisite intent and the requisite knowledge. The requisite intent is intent to cause the modification of the contents of any computer and by so doing:

- to impair the operation of any computer;
- to prevent or hinder access to any program or data held in the computer; or
- to impair the operation of any such program or the reliability of any such data.

Technical Control

Lack of adequate technical and administrative control has been a barrier to e-government in Africa. Security is a critical aspect of achieving successful e-government in West Africa. In Nigeria for example, the Central Bank holds for all the commercial banks in the country. The Central banks has central database, run by government administration, which is under the control of Federal Ministry of Finance. Many employees are in the habit of not protecting their passwords by writing them on a sticky note and pasting it on their computer, while others forget to sign off their computer at the end of workday. It is very important that government ensure that sensitive information is protected as well as the network and server well secure. Technical and Administrative control must put in place for e-government to succeed. The technology of digital signatures, encryption, authentication, firewalls, and intrusion detection systems coupled with the use of administrative control such as background check, data classification, audit and standard make the promises of e-government reasonable and achievable.

Digital Signature

Digital Signature is needed to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. In Nigeria many outgoing message or document are being digitally because of various forged documents associated with Nigeria National Petroleum Corporation and Central Bank of Nigeria with reputable certificate authority. The most common certificate authority used in Nigeria and Ghana is VeriSign and Web Trust.

Encryption

Encryption is the process of converting data from a plain text or readable form into a cipher text or unreadable form. Only the intended recipient could read this message based on the knowledge of the key to the encrypted message. Many frauds committed in Africa are online based. In Nigeria and Ghana online banking application is the most vulnerable to the attackers due inadequate security of either network or application. They gain access to customer's account through online transactions or gain access to banks database and steal most valuable documents from the bank such as banks business forms use for fraudulent activities either within the country or outside the country.

Firewall

Firewall is the protection of computer network from intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device or software program on secure host computer. The firewalls will serve as middlemen to inspect messages before delivering them on to the network. If they receive any unauthenticated packets, the incoming connections will be terminated immediately. Only if the connection knows the password or if it's authorized then the network will be open to the user. A firewall hides the Internet-connected computer from view, it can block and hide ports and prevent port scanning used by online criminals to attack. There are different types of Firewalls. There are simple firewalls capable of blocking only ingoing connections. This is not good for commercial base applications such as government application or banking applications because it has only limited protections and it is to break in by hackers. There are many advance firewalls that come with pre-set rules. The rules could be customized for each government or banking application for traffic filtering. The new trend in firewall now is that some vendors are integrating firewall into application, Web ACL, Instant messenger, Email, Integration with In-line IDS and anti-virus software in low-end boxes. This will be a great tool for developing nations that just entering the world of Internet. Though, many African countries use Cisco firewall and Symantec firewall for the government applications and portals.

Anti-virus

Anti-Virus protection is another issue that must be addressed by the government. Because of the nature of e-government, government entities must ensure that users are not accepting e-mail from unknown sender or open any email that look suspicious to them. Fingerprint based anti-virus software, must be installed that will compare signatures to its virus database which will determine whether the e-mail or file contains malicious code in it. It will also create a log that will assist in identify threats against the network. The anti-virus that are commonly use in West Africa in particular are AVG, which is the real-time protection against viruses and spywares. Avast protect computer in real-time against viruses, spy wares, mal-wares. Avira is a scanner that detects virus and malwares base on virus behaviors. PCTools Antivrus protect against viruses, worms and trojans in real-time with a very active heuristically scanner.

Spyware

Spyware and Ad-ware are another threat that must be protected against though they are probably more passive than any other types of threats, but just as dangerous. These items are usually added on the network without the user knowing the presence of the threat. So to protect government portal against these threats, government should install a web blocking programs on all employee workstation such as Surf Control to block users from going to networks that the company has deemed unauthorized. When users go to one of these sites, they will receive a message that says "Access Denied, followed by some explanation.

Intrusion Detection

Intrusion detection system is great way of monitoring network traffic and monitors for suspicious activity and alerts the system or network administrator. It monitors the network for bad behavior, but also collect and analyze data that can be helpful in determining what is considered normal network behavior. It is very important for Systems Administrators to understand their network activity, not just when it's under attack from the outside world, but also what is considered acceptable daily activity from its own end users. The IDS can be configured to create log files of all network activity that will be placed in the government permanent security file. If the Intrusion Detection System notices suspicious activity or abnormal behavior on the network, it will sound an alarm that will notify the System Administrator immediately or block the user or source IP address from accessing the network and the information gathered from analysis may use to prevent future attack or use to prosecute the attacker.

Administrative control

Administrative control can use content filtering web proxy server over the content that may be relayed through the proxy. It is commonly used to ensure that Internet usage conforms to acceptable use policy. The content filtering proxy will often support user authentication, to control web access. It also usually produces logs, either to give detailed information about the URLs accessed by specific users, or to monitor bandwidth usage statistics. It may also communicate to daemon based and/or Internet content adaption protocol (ICAP) which is hypertext transfer protocol (http) anti-virus software that will scan or filter data for security against virus and other mal-ware by scanning incoming content in real time before it enters the network.

The common methods used for content filtering include: URL or DNS blacklists, URL filtering, MIME filtering, or content keyword filtering. Our server will employ content analysis techniques to look for traits commonly used by certain types of content providers.

An intercepting proxy server (also known as a "transparent proxy") combines a proxy server with a gateway. Connections made by client browser through the gateway are redirected through the proxy without client-side configuration (of often knowledge).

Intercepting proxies are used to prevent avoidance of acceptable use policy, and to ease administrative burden, since no client browser configuration is required.

The components of the network will consist of several like computers connected using Ethernet switches, routers and firewalls. The combination of routers, firewalls and file servers will be used to detect and alert of intrusion detection, authenticate, authorize, and provide access to the corporate information and data, and scan for viruses, Trojans, spy-ware, and other mal-ware.

Access Control Policy

Access control is used to identify and grant certain privileges to information. It consists of authentication and authorization. Authentication and authorization is a big issue in Africa, there are no policies for authentication and authorization process. There are no checks and balances by the government, the privileges are been granted indiscriminately in regard to authentication and authorization. Some employees have same privilege to the database like a database administrator. The privileges given are not based on the role the employees performed base on the level of the seniority. Many banks and government offices are located in rural area of the country; these employees connect to the server through remote login. If the network or server is not firmly secure or protected, the network can be expose to virus or attack.

Employee access to the bank network or government server from rural area can be gained through two ways, either access through the proxy servers or from the quarantine network. Remote login users or citizens from home will access to the network using the Remote Access server or the quarantine network's RADIUS server. Once the Remote Access server (RAS) grants permission to continue on to the network, the Remote Authentication Dial In User Service (RADIUS) server will send a request to the Network Access Server (NAS) to gain access to a particular network resource using the access credentials. Once authenticated, Radius determines what rights or privileges the person or computer is authorized to perform and makes a record of this access in the accounting feature of the server

The second option of access to the network or server by the remote offices will to bypass the Remote Access Server and enter directly into the quarantine network connecting to the RADIUS server. The remote access server will scan the remote user's computer for the presence of virus infections, Trojans, worms, spy-ware and other mal-ware before allowing them access to information.

The government should invest in the professionally skill staffs to manage their ICT resources such as system administrator, Information security staff and other IT staff. Granting privileges to access the network and servers and systems indiscrimately should be stopped. Individual and unique logins must be created to authentication users and use of passwords, smart cards, biometrics, or other recognized forms of authentication should be use in government application or in the banks.

Legislative compliance

African countries are self-regulated and many of them are struggling with their regulatory body. The region has many local regulations that are not capable of handling today's global cyber enemies. The local regulation may not be the best practice to protect electronic transactions and personal information because these criminals are from all over the globe.

In 2005, Federal Republic of Nigeria sponsored a bill, Computer Security and Critical Information Infrastructure Protection Bill (otherwise known as the Cyber crime Bill)[14]. The Cyber crime Bill aims to "secure computer systems and networks and protect critical information infrastructure in Nigeria by prohibiting certain computer based activities" and to impose liability for global crimes committed over the Internet. The Cyber crime Bill will require all service providers (telephone and internet) to record all traffic and subscriber information for such period as specified by the President, and to release this information to any law enforcement agency on the production of a warrant. Also, in South Africa a similar legislation was passed. Electronic Communications and Transaction Act of 2002[4], and the Law Commission Issue Paper on Privacy Public Service Act and The Convergence Bill which is now called The Electronic Communications Bill. Since Africa nations cannot formulate an effective legislation that will international accepted, they could as well adopt the widely use international legislative body such as:

- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes Oxley Act (SOX)
- Personal Data Act
- Computer Misuse Act

The Financial Modernization Act of 1999, Gramm-Leach-Bliley Act (GLBA). GLBA is a provision to protect consumers' personal financial information held by financial institutions. Specific components of GLBA include The Safeguards Rule, which requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule mandates that financial institutions develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. This Act ensures that financial institutions protect their customers' information. It makes financial institutions take a closer look at how they manage private data.

Sarbanes-Oxley Act

In 2002 President George Bush signed the Sarbanes-Oxley Act into law to "re-establish investor confidence in the integrity of corporate disclosures and financial reporting" The act was brought on by the large number of corporate financial fraud cases (such as those of Enron, WorldCom, Tyco, Adelphia, AOL, and others) and by the end of the "boom" years for the stock market. Each company's external auditors must also audit and report on the internal control reports of management and any other areas that may affect internal controls. The Act requires all public companies to submit both quarterly and annual assessments of the effectiveness of their internal financial auditing controls to the Securities and Exchange Commission. The details of the Sarbanes-Oxley Act address many of the tactics companies have used to "cook the books" over the years. The company's principal executive officer and principal financial officer must personally certify that the financial reports are true and that everything has been disclosed. The Act's provisions apply to all companies, United States and foreign companies, but this Act has been adopted by many industrialize countries. African countries should adopt this

Act which will solve many of their financial mismangement and corruptions. The Act requires all public companies to submit both quarterly and annual assessments of the effectiveness of their internal financial auditing controls to the Securities and Exchange Commission. The details of the Sarbanes-Oxley Act address many of the tactics companies have used to "cook the books" over the years. In the next few sections, we'll go over some of the more popular methods of improving a company's bottom line

Emerging technologies

Emerging technologies is a new security technology to combat Internet and application threats. This includes, built-in biometrics, USB authentication tokens and self-encrypting hard drives.

Built-in biometric

Built-in biometric is a biometric-based encryption and decryption device that uses fingerprint scanners, it adds layer of protection by directly linking the fingerprint image to the system Basic Input/Output System that makes it harder for any hacker to break into the system. Using biometrics for personal authentication is very accurate but is it will very expensive for African government to implement considering the state of their economy.

USB authentication

USB authentication allows the user to plugs in the device, enters a password, and gains access to the application or network. Through this device it is possible to monitor access during the entire period a user is logged on. This makes it possible to track activity more accurately and prevent unauthorized use. The administrators can store multiple codes on the same device, thereby fortifying protection for restricted applications and files.

Also, the devices can handle two-way authentications**,** both private keys and digital certificates within the same token that allow the user to work securely from any PC. This is good for government officials that are constantly traveling out of country for seminars or government offices that are located in a remote part of the country that needs access to government applications remotely. It is inexpensive and easy to use.

Self-encrypting hard drives

Self-encrypting hard drives technology encrypts and decrypts automatically all data written to the disk. It makes data inaccessible to anyone who lacks the correct password when the computer first starts up. It is easy to use and eliminates the pressure of forgetting to encrypt the data.

E-government Access issues

Access to Information and Communication Technologies infrastructure is very crucial to e-government all over the world. Many African countries are facing low Internet penetration because of the lack of infrastructure to Access the Internet. Some of the problems are shortage of computers, high cost of interconnectivity, poor electricity. These have been major barriers to successful take off e-government in African countries. According to World Internet Stat 2008, (table1 below) Africa with population of 975,330,899 is the second biggest continent beside Asia with population of 3,780,819; only 54,171,500 of the population can access the Internet, which means only 5.6 percent of the Internet access which is below the world average of 23.8 percent. Low Internet access could be also attributed to high-level poverty in the region with corruption and mismanagement

INTERNET USERS AND POPULATION STATISTICS FOR AFRICA						
AFRICA REGION	**Population (2008 Est.)**	**Pop. % in World**	**Internet Users, Latest Data**	**Penetration (% Population)**	**Use Growth (2000-2008)**	**% Users in World**
Total for Africa	975,330,899	14.5 %	**54,171,500**	5.6 %	1,100.0 %	3.4 %
Rest of World	5,734,698,171	85.5 %	**1,527,400,089**	26.6 %	328.5 %	96.6 %
WORLD TOTAL	6,710,029,070	100.0 %	**1,581,571,589**	23.6 %	338.1 %	100.0 %

Table 1

Shortage of Computers

Shortage of Computer is one of the major issues facing the advancements of e-government development in Africa. Computer is needed to be able to access government portal for payment of tax, electricity bill and apply for jobs. According to the UN studies in 2006, Africa has an average of 100 people to one computer[10]. Many African citizens cannot afford to buy personal computer or laptop to access the Internet because high price tags on these computers. This has been major hindrance to successful take of e-government in Africa. African government should make computer affordable the citizens by eliminating the import tariffs and reduce import license fee.

High cost of Internet connectivity

Internet connectivity is extremely expensive when you compare to Western countries especially with the average median income, most people in Africa do not subscribe to any Internet usage because of high cost of Internet connectivity which has bee a constraint to e-government and economy as a whole. In Nigeria and Ghana, government for Internet access at the post office for a few token and better still some travel far and wide to place where Internet is free such as school, Library and some other public Internet access. Churches and Mosque has a community center available for the members for emails and jobs access. Wealthy families go to the Internet cafes, kiosks, community telecentres and community phone-shops for Internet access at very high price. As you can see from (Figure 4) below, the Internet café was crowded, the cost of Internet per one hour is $4 in Nigeria and Ghana and in South Africa it cost $3 per

Internet café in Africa

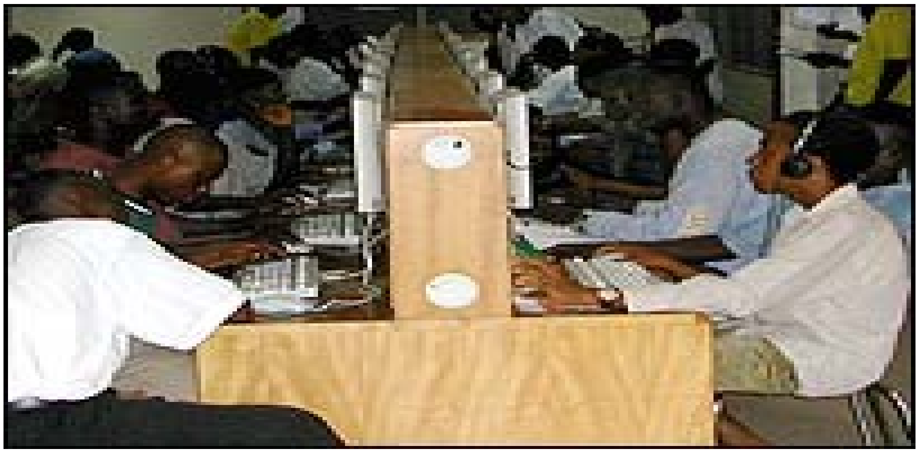


Figure 4. Goggle Image.

Poor Electricity

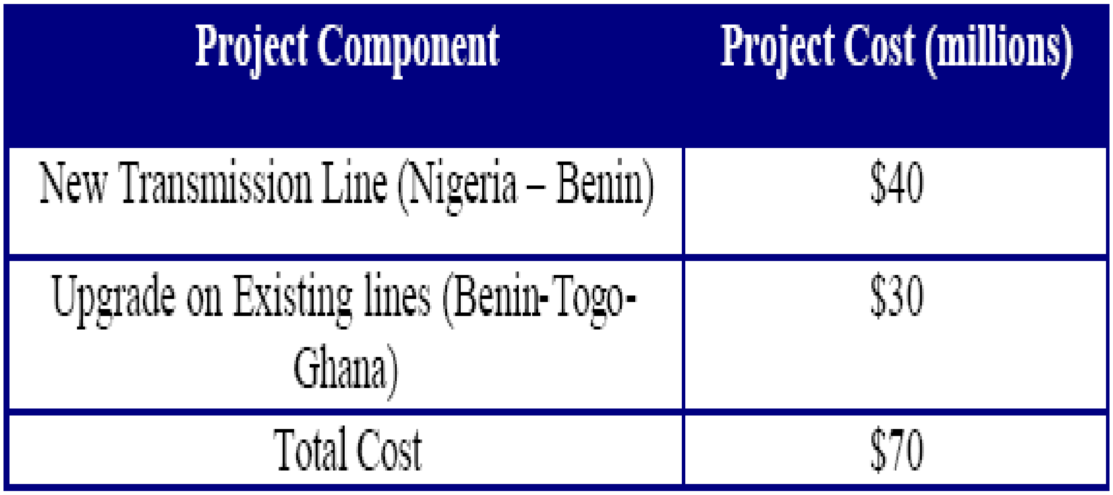
Electricity is a luxury commodity in Africa countries especially in West African region. In Nigeria for example, the bulk of power plants and transmission facilities was built in the 1950s and 1960s during the colonial era. The failing economy in West Africa is largely to blame on government monopoly of social services, no private investors was allowed to invest in this social infrastructures. As a result of failing electricity citizen look for alternatives energy such as generators to power their homes or business, which is extremely expensive. The effect of generator to power business increases the business overheads and this lead to increasing the cost of productive and thereby increase the price that consumer pay for the products or services. Africa countries are blessed with many resources to power their electricity. They have uninterrupted sun supplies for eight to ten hours most of the day which could be use to create solar energy, they are surrounded by sea, rivers, lakes and dams hydroelectricity and also, Nigeria is blessed with gas for bio-gas power. It is time now for African government to pull their heads together to solve the problem of electricity whether as continent or as a region.

In October 2000, 14 members of the Economic Community of West African States (ECOWAS) Africa Renewal, Vol.18 #4 (January 2005)[15] signed an agreement to launch a project to boost power supply in the region. Under the West African Power Pool (WAPP) agreement, countries hope to develop energy production facilities and interconnect their respective electricity grids. According to the agreement, the work would be approached in two phases. The first involves countries already interconnected, including Nigeria, Benin, Burkina Faso, Ivory Coast, Ghana, Niger and Togo. The second phase involves countries not yet connected: Gambia, Guinea, Guinea-Bissau, Liberia, Mali, Senegal and Sierra Leone. Countries will work to harmonize the regulatory frameworks that govern their electricity sectors. ECOWAS estimates that 5,600 kilometers (km) of electricity lines connecting segments of national grids will be put in place.

In 2000 ECOWAS estimated the cost of completing the major interconnecting trunk lines between Nigeria, Benin, Togo, and Ghana will be $ 70 Million [11] (see table 2 below). The project costs are split into the two project components: (1) construction of the new transmission line from Nigeria to Benin; and

(2) Capacity expansion of the existing transmission lines from Benin to Togo to Ghana. The total is transmission 330KV line and total length of 70km from Ikeja (Nigeria) to Sakete (Benin) to Lomé (Togo) and Tema (Ghana) (see table 3 below).

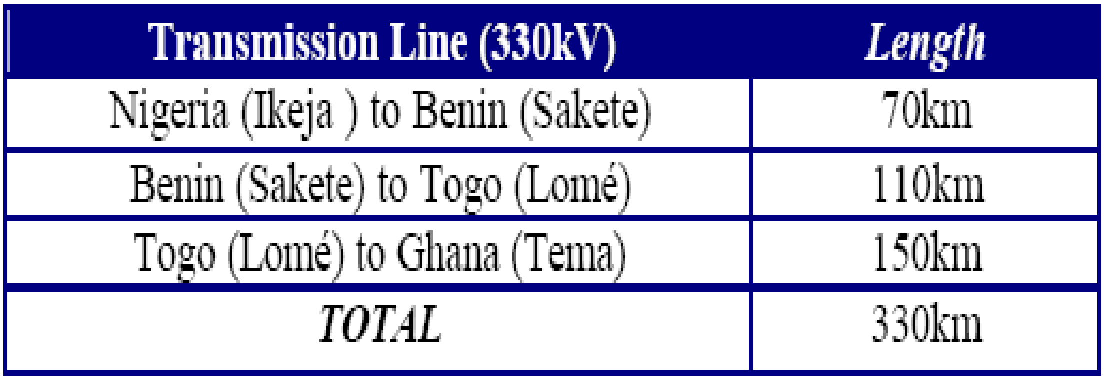
West African Power Pool Project



Project Component	Project Cost (millions)
New Transmission Line (Nigeria – Benin)	$40
Upgrade on Existing lines (Benin-Togo-Ghana)	$30
Total Cost	$70

Table 2.

West African Power Pool Project



Transmission Line (330kV)	*Length*
Nigeria (Ikeja) to Benin (Sakete)	70km
Benin (Sakete) to Togo (Lomé)	110km
Togo (Lomé) to Ghana (Tema)	150km
TOTAL	330km

Table 3.

Internet Penetration

Internet penetration in Africa remains the lowest in the world. The low penetration can be largely attributed to high cost of broadband connectivity and shortage of fixed-line telephone. The telephone fixed line dialup connection is very (figure 5 below) Africa has average of 3 telephone lines per 100 habitants but whereas in United State 33 telephone fixed line per 100 habitants[10]. Many countries in Africa are still using analog telephone services, which are very outdated and slow in connection. The Internet broadband or DSL market is under penetrated due to high cost of connectivity. The average cost of broadband Internet is $150 per month. There are fewer broadband providers in the region due government limitation on the number of providers. Before the explosion of cell in Africa, government has been sole provider of the telecommunication system. No private investors were allowed to own part of the phone business in Africa. The fixed-line was managed and maintained by government workers.

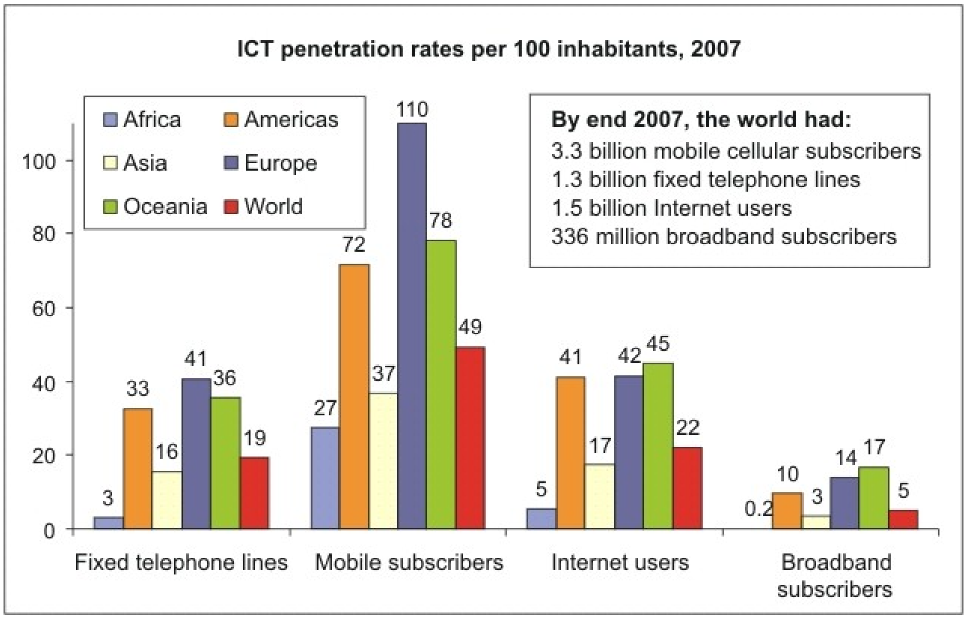


Figure 5.

In 2002, there was explosion of mobile phone in Africa through GSM network, which accelerated the fast growth of the mobile sector especially in Nigeria. These mobile phone businesses continue to flourish throughout the region, while the fixed-line was abandoned. This forced government to liberate and privatize the telecommunication system and end the monopoly of the telecommunication era. Despite the explosion of the mobile phone, Africa is still having lowest Internet penetration in the world.

In 2006 Internet users penetration (figure 6 below) Africa has Internet users penetration average of 4.8% of Internet penetration compared with the world average of 17.2. Taking the population of Africa into consideration, this means that 4.8 percent of the inhabitants were using Internet. With recent government liberalization of telecommunications, many investors was attracted to the region to invest in the telecommunication infrastructure, the African will soon be enjoying broadband access. West Africa region is expected launch its submarine fiber-optic cable in 2009 to have direct access to fiber optic based international bandwidth to supplement her current SAT-3/WASC the only international fiber optic serving the African West coast.

Internet users penetration by region

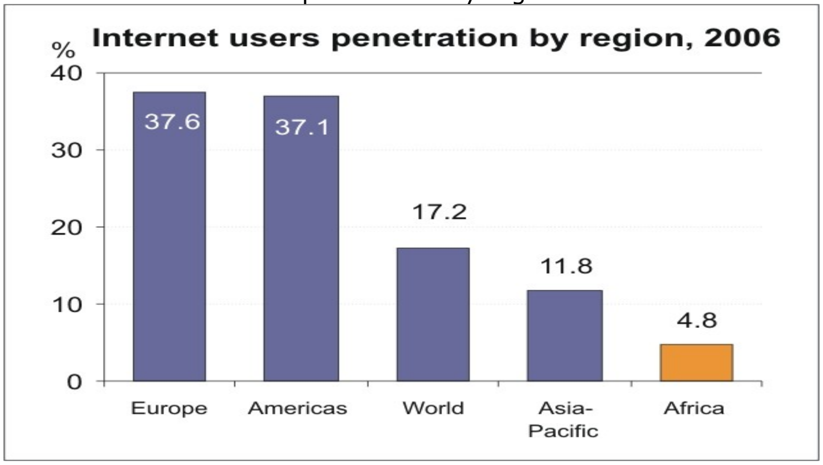


Figure 6.

Lack of peace and stability

Civil war and unrest have wiped away telecommunication infrastructure in some African countries that are ravaged by war. In Liberia, Sierra Leone and Somalia, the war has left most fixed-line telephone non-operational in this region. They are the poorest countries in Africa today. Because of the unrest, investors are not attracted to invest in and build the telecommunication infrastructure like other African countries that attract many investors.

Readiness for E-government

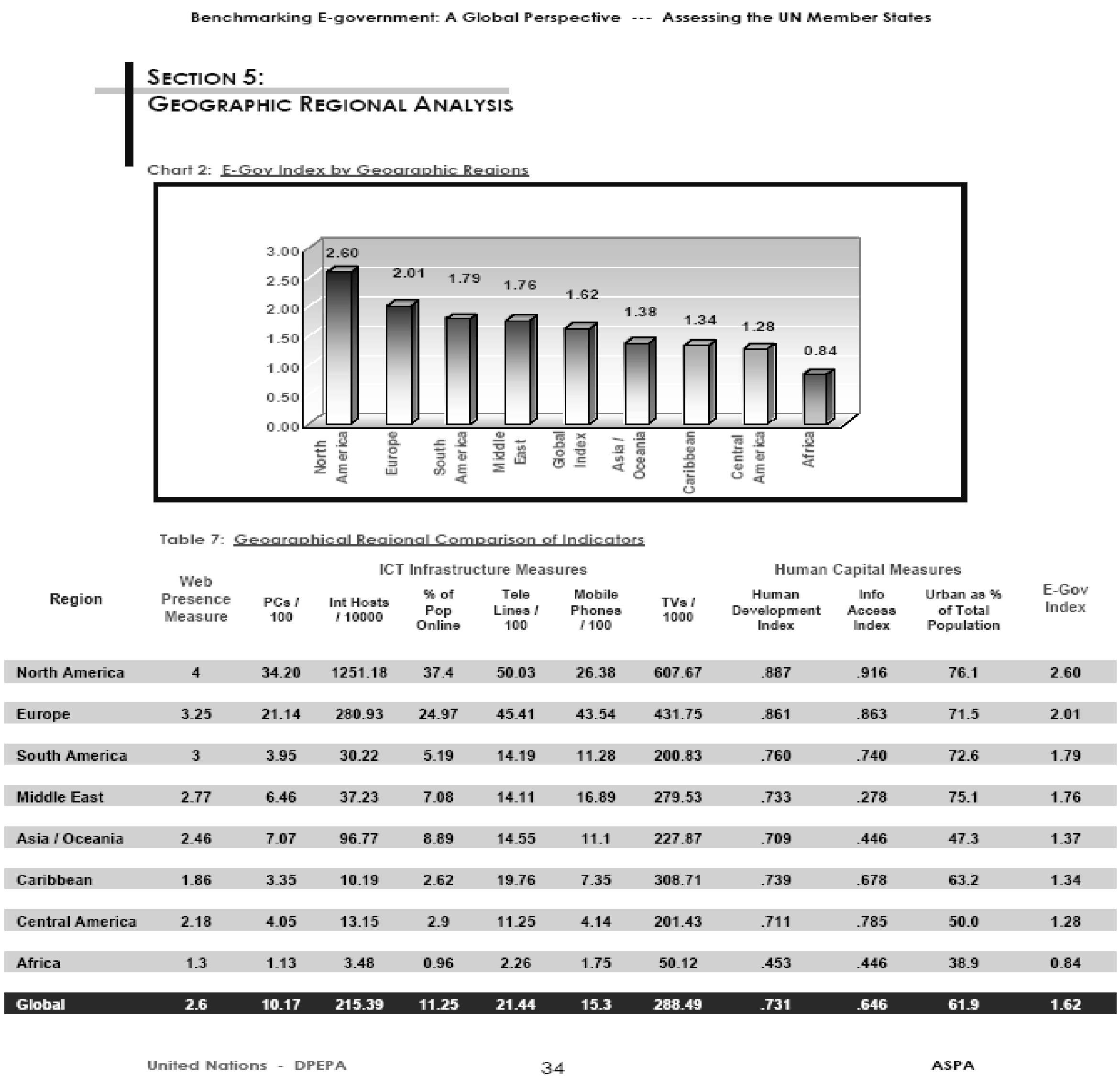
E-government readiness is the preparedness of a country transformation from traditional government service to electronic government. E-government readiness is directly attributed to availability of telecommunication infrastructures, human resources and financial resources development of a country.

Human Resources

Human resource development is very essential in taking full advantage available in the new global information based economy. One of the major set backs in e-government program in Africa has alack of skill labor, which is crucial to management of e-government services. For e-government to be in the state of readiness, there must be availability of human resources. Human capital development is an essential ingredient of e-government. In the past Africa nations has experienced exodus of professionals to the Western world for better life. For many years now education has been neglected due to poor economy, political instability and civil war. The schools are been neglected, high rate of young kids have dropped out schools and leads to high level of illiteracy. Teachers are not been paid for months of salaries for lack of funds from government. Schools were been closed for months due to Teachers and students strides. Many professors left the teaching job to find another profession because of persistent of non-payment of theirs and constant government educational policy changes. The professors earned less than their counter part that took government administrative jobs. The school infrastructures are very old and there are no books in the libraries and some of the books are old dated back to the time of colonial eras. The curriculums are very old and do not reflect the current changes in world. There are few computers in the school with outdated hardware and software. Many schools are overcrowded with few infrastructures to work with and teachers are not well paid compared with their counterpart in advanced countries.

In 2005 United Nation global perspective on member states (see table 4 below) on e-government readiness, Africa scored the lowest of the index 1.62 in overall index compared with global average of 2.6. On Human Capital measurement development index (see table 4 below) Africa scored .453, the world average is .731. The overall score in human capital development is in deficiency stage[8]. Africa lack the technical skill workers that are required for the successful takeoff e-government. In Nigeria for example, some Universities are not offering computer science programs due to lack of telecommunication infrastructures such as computers, telephone lines and Internet access.

E-Government indices on ICT Infrastructure and Human Capital Measures



SECTION 5:
GEOGRAPHIC REGIONAL ANALYSIS

Chart 2: E-Gov Index by Geographic Regions

3.00
2.50
2.00
1.50
1.00
0.50
0.00
2.60
2.01
1.79
1.76
1.62
1.38
1.34
1.28
0.84
North America
Europe
South America
Middle East
Global Index
Asia / Oceania
Caribbean
Central America
Africa

Table 7: Geographical Regional Comparison of Indicators

Region	Web Presence Measure	ICT Infrastructure Measures						Human Capital Measures			E-Gov Index
		PCs / 100	Int Hosts / 10000	% of Pop Online	Tele Lines / 100	Mobile Phones / 100	TVs / 1000	Human Development Index	Info Access Index	Urban as % of Total Population	
North America	4	34.20	1251.18	37.4	50.03	26.38	607.67	.887	.916	76.1	2.60
Europe	3.25	21.14	280.93	24.97	45.41	43.54	431.75	.861	.863	71.5	2.01
South America	3	3.95	30.22	5.19	14.19	11.28	200.83	.760	.740	72.6	1.79
Middle East	2.77	6.46	37.23	7.08	14.11	16.89	279.53	.733	.278	75.1	1.76
Asia / Oceania	2.46	7.07	96.77	8.89	14.55	11.1	227.87	.709	.446	47.3	1.37
Caribbean	1.86	3.35	10.19	2.62	19.76	7.35	308.71	.739	.678	63.2	1.34
Central America	2.18	4.05	13.15	2.9	11.25	4.14	201.43	.711	.785	50.0	1.28
Africa	1.3	1.13	3.48	0.96	2.26	1.75	50.12	.453	.446	38.9	0.84
Global	**2.6**	**10.17**	**215.39**	**11.25**	**21.44**	**15.3**	**288.49**	**.731**	**.646**	**61.9**	**1.62**

Table 4.

Government should stop import tariffs on computers and its components for educational purposes. Government should lay down extensive programs to promote higher training, and development for its citizens in the private and public sectors to boost human capital. Government should increase educational funding to train citizen in ICT and related studies. There should be new curriculum that put into consideration the ICT in Primary and Secondary Education for early understanding of information technology. To be able to compete in digit world, college curriculum must be redesigned to accommodate science courses for the training of ICT professionals. Government should make funding of ICT training of both secondary and post secondary education a priority. Private citizens should be encouraged to open training centers for low fees in computer training.

Telecommunications infrastructure

For a country to be in state of readiness there must be adequate Telecommunication infrastructure, availability of personal computers and easy access to Internet. Telecommunication infrastructure is a pressing issue in African nations. There are several reasons for the inadequate telecommunications infrastructure and lack of public access to the Internet which including inadequate personal computers, inadequate telephone line and lack of broadband access for Internet connection is still a major barrier in Africa. The high cost of computers, hardware and software represents another serious impediment to e-government in Africa. Low Internet penetration has to do with the lack computers because it is very expensive and is not within the reach of average citizen. The new computer cost between $1500 and $2000 and used between $900 and $1500.

In many countries, telecommunication infrastructure is a luxury items, which is beyond the reach of the citizens. In Nigeria and Ghana, computer and internet access could be found in elites homes and working class people but ordinary citizen could not afford to buy or subscribe to internet due to high price, some pay as much $200 to $250 a month for Internet when the average salary is about $150 a month. Likewise, many African countries maintain trade barriers to importation of information technology accessories making it difficult for both merchants and customers to purchase the computers and information systems they need to access the Internet. In Nigeria importation of computers, cell phones and its accessories is deem to be a luxury items and it attracted high import tariffs between 35 and 50 percent depending on the category, this raise the cost beyond the reach of the majority of the populations. Absence of telecommunication infrastructure is part of the reason why cost of running business is expensive in the Africa when compared to other regions.

Inadequate bandwidth is another telecommunication issues that affect the progress of e-government. Bandwidths are very expensive, limited in number and is been oversold by service provider to too many users, so the network becomes over crowded, unstable and slow download speed. Telephone fixed line dialup services are unavailable and unreliable. The reason high cost of bandwidth is due to government monopoly, the licensing criteria to allow this technology into the country is excessive and over-regulated and the to contain it to one service provider. Many African countries access the Internet through various channels, VSAT, Wimax, Dial-Up and so on. VSAT, Very Small Aperture Terminals allows delivery of Internet connectivity via satellite, while WIMAX (Worldwide Interoperability for Microwave Access) is an alternative to cable and DSL and allows broadband access anytime, anywhere provided it is within the coverage area of the base stations. Dial-Up involves the use of telephone lines to connect to the Internet. Bandwidth is limited It is one of the major reasons for poor Internet service in the country. Africa countries are interconnected either by a combination of radio relay links, open wire lines, radiotelephone stations, satellites, microwaves, fixed local loop installations and substantial mobile cellular networks.

In North African region (Egypt, Tunisia and Algeria) are connect by undersea fiber-optic cable called SEA/ME/WE-3. SEA means South East Asia, ME means Middle East and WE-3 means Western European (Germany, England and France). They have 39 landing points in 33 countries and 4 continents from Western Europe (including Germany, England and France) to the Far East (including China, Japan and Singapore) and to Australia.
In South region, they have two segments submarine cable system; called SAF (South Africa Far East) which links Malaysia and India.
In the East to South Africa via Mauritius and Reunion and SAT-3/WASC (South Africa Trans-Atlantic.
In the West, they have WASC (West Africa Submarine Cable), which continues from South Africa Portugal and Spain, which landed in many of West African countries (see figure 7 below).

African undersea cable line

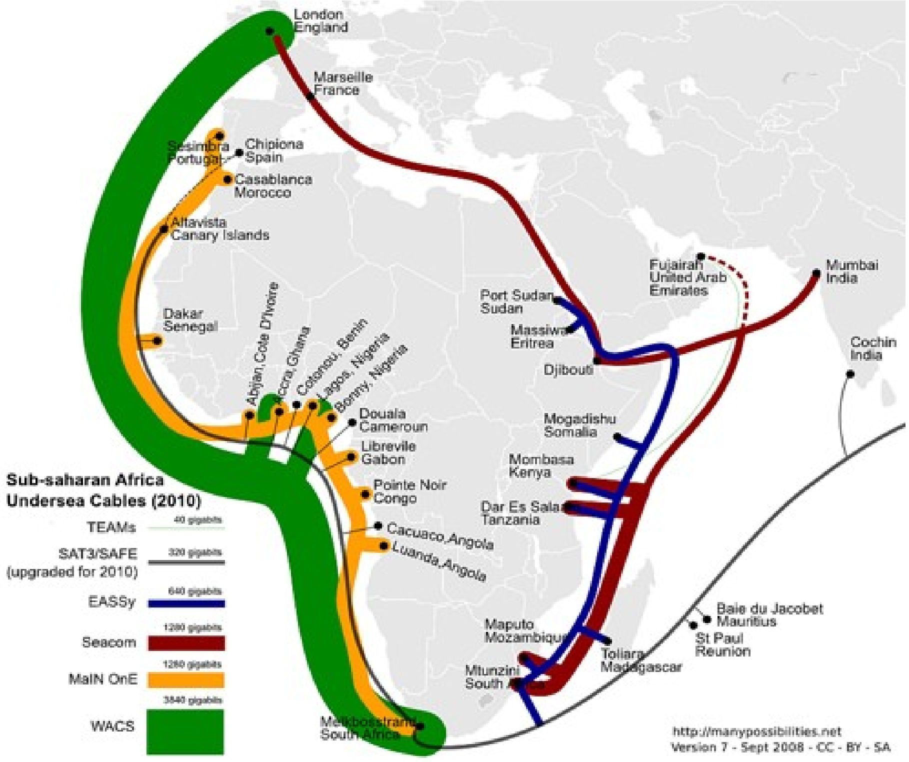


Figure 7.

In 2007 Nigeria launched its own satellite communications, which is called NIGCOMSAT. With launching of NIGCOMSAT, broadband Internet access has become easier and more reliable for Nigeria people and the neighboring country. Many schools and rural area will now able to connect to the Internet with minimal problems and this also has increased the Internet penetration by 40 percent of the populations.

Wireless cellular is becoming one of the most common forms of communication means in the rural Africa nations. The deregulation and privatization of the telecommunications sector led to investment by Global System of Mobile Communications (GSM). The leading mobile telephone providers in Nigeria are MTN, V-Mobile, Globacom and Mtel. Africa has experienced tremendous growth in the mobile services market. The mobile phones providers also that Internet access on the mobile phones. In Nigeria, (see table 5 below) the mobile phone subscribers grow from 0.02 million in 1998 to 44 million in 2008. This is a tremendous growth of 33 percent within ten years.

Mobile subscribers and penetration rate in Nigeria

Year	Subscribers (Million)	Penetration
1998	0.02	0.02%
1999	0.03	0.02%
2000	0.04	0.03%
2001	0.35	0.28%
2002	1.46	1.15%
2003	3.35	2.49%
2004	9.39	6.85%
2005	18.4	13.2%
2006	29.1	20%
2007	41.6	29%
2008 (Mar)	44.4	31%

Table 5.

Financial Resources

Africa is blessed with many natural resources such as crude oil, cocoa, coffee, tobacco, tea, gold, diamond and prescious stone, they are still the proorest in the world. African nations have a very low income per capita and this affect their financial relationship with developed world. Poor economic performance and poverty are seen everywhere in Africa and there is no doubt that without heavy investment in infrastructures it will be very difficult for Africa to make any progress towards the e-goverment. African government have been confronted with many challenges. The South faces tremendous problem of HIV/Aids with the memory of aparthatid not farway; the Eastern region faces the problem of war; HIV/aids and pirates; Northern faces the problem of terrorism and political unrest and Western problem is civil war corruptions. Due to this inherent problems,it is quite difficult for the region to raise large amount of capital from foreign investors. Due to financial constraint the telecommunication project is been neglected and more often abandoned due to limited working capital needs to complete the projects.

Training

Many African countries, lack adequate skill ICT, In Ghana and Nigeria for example, many of the high- skill professionals such as software developers, system engineers, communication and network engineers left the country for better pay overseas. The consequence of this brain drain is the shortage of skill ICT professionals in the region. Human resources is the main factor for economic prosperity and developments of a country, training of ICT professional should be the government priority for this digital age. Majority of the colleges and schools do not have enough teaching professionals to teach ICT in schools and where there are teachers, there are inadequate computing infrastructure, such as computer laboratories, personal computers and internet access to facilitate teaching and learning.

Government should focus on training of ICT teachers to teach in schools and colleges. The School curriculum should be redesigned to accommodate new development in technology. Salaries of teachers and professors should be increased to match their counter part in advanced countries. ICT educational infrastructures such as multimedia computers, peripheral equipment, software and telecommunications should be eliminated. Community volunteers must be encouraged to training citizen on how to use computer and Internet. More youth should be encouraged and attracted to studies computer science. More classrooms like those shown in Figure 6 and Figure 7 should be established.

Students during a TanEdu hands-on computer course

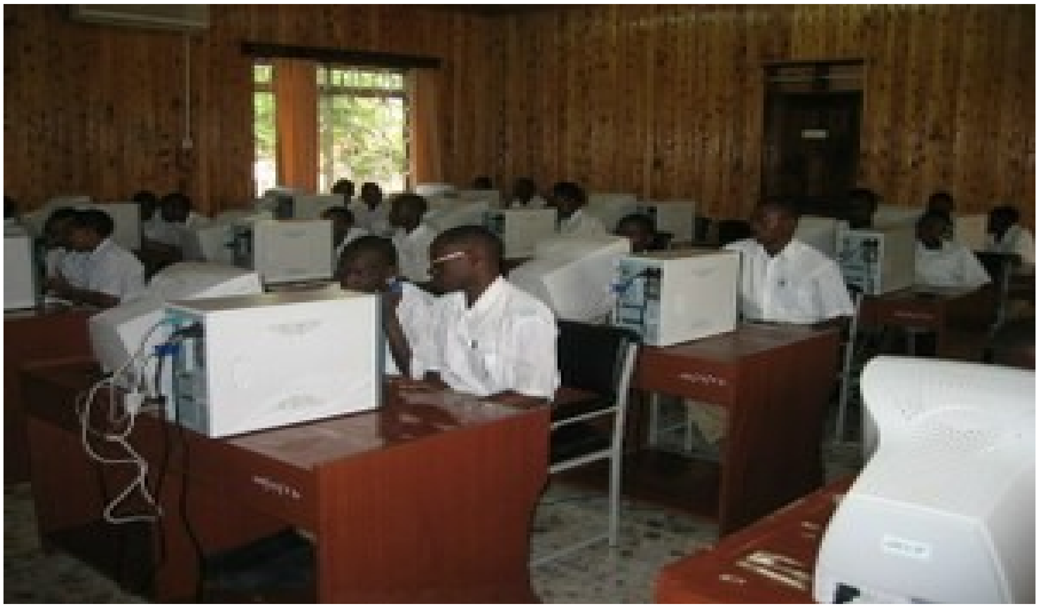


Figure 6. Source: Tanzania Department of Education

Youth at the community center for computer lesion

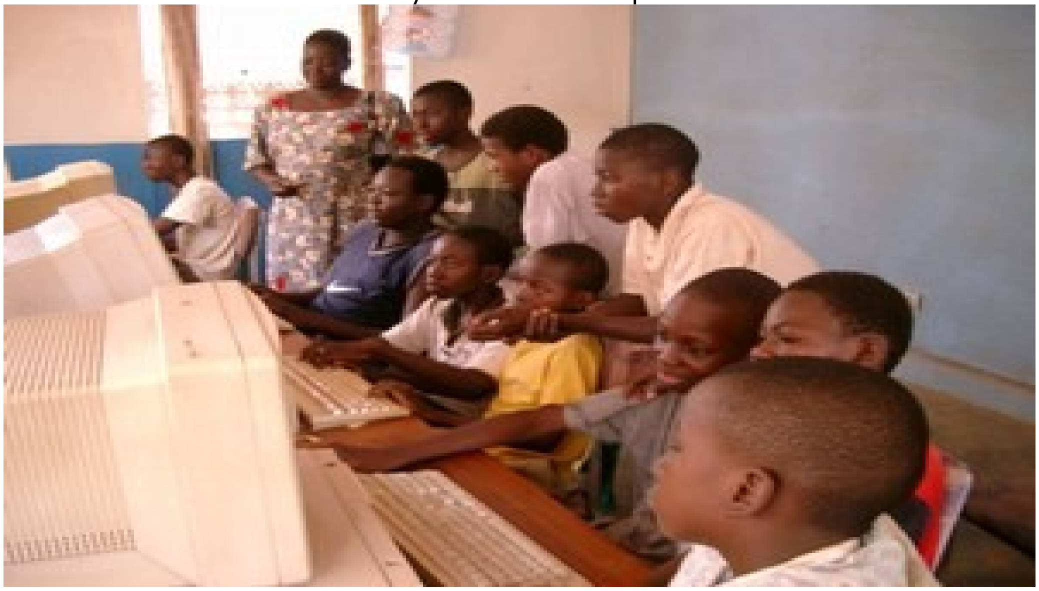


Figure 7. Tanzania Department of Education.

Conclusion

E-government is an electronic government or Internet-based government that uses electronic technologies to exchange information and and to provide services for citizens, businesses, and other arms of government. There are many benefits of government to both the citizen and government. The citizens could pay their bill online, change address, purchase stamps online, file their taxes, apply for jobs and view government announcements, information, programs and school information.

The government could also benefits by collecting thier revenue ontime through online payment center for the citizen and businesses. The judicary, legslature, and administration will also benefits from the e-government. The rural area will benefits from e-government programs through the rural area internet center where they can check government websites for information needed for development.

As there are benefits so also the challenges that associated with the e-government. Such challenges include privacy issues, security issues, access issues, policy issues and complinace issues. Government should develop policies and legislation to ensure that public valuable information is protected. African governments should join with global alliance to fight the cyber crime because cyber crime is a global problem. Government must secure data, applications and networks firmly to prevent unauthorized access to the information.

There are many emerging technologies that could to prevent unauthorized access or hackers from their networks such as firewalls, encryptions, anti virus digital signature, spy ware, intrusion detection, biometric and self-encrypting hardware. The success of e-government is how ready the country is. Telecommunication infrastructure such as telephone, computers and bandwidths must be adequate and available for the citizen making any sacrifices. Without electricity, Internet cannot function, and with the Internet the public cannot access the government web portal for information. There must be availability of electricity in the country. Human resources must be adequate and available at all times.

Telecommunication require skilled professional, government must invest on training of ICT staffs, teachers to teach ICT in schools and professors to teach colleges. There must be e-government awareness training in both urban and the rural areas. Government must establish Internet centers especially in the rural and remote area for citizen who will not otherwise subscribe to Internet.

Schools, community centers, libraries and elderly centers must be equipped with Internet.

References:

1. Zhiyuan Fang, E-government in Digital Era: Concept, Practice, and Development, International Journal of The Computer, The *Internet and Management, Vol.10, No.2, 2002,* pp. 1-22. Retrieved May, 2, 2009

2. Dooley, Brian J. (2004). Telecommunication in Africa. Retrieved 2/19/2009 from the http://www.faulkner.com/products/faulknerlibrary

3. Heeks, Richard. E-government in Africa. *Promises and practices,* IDPM, University of Manchester, 2002. Retrieved April 15, 2009

4. South Africa. Department of public service Administration. South African E-government: 31 October 2005. 19 Feb. 2009.

5. International Telecommunication Union (ITU) (2004), Activity Report Year 2003, Africa Region. Retrieved 03/29/05 from http://www.itu.int/ITU-D/afr/AfricanActivityReport/documents

6. United Nations, Department of Economic and Social Affairs *Global. E-government Readiness Report.* New York, 2005. 13 April 2009.

7. ITU, *World Telecommunication Development Report: Access Indicators for the Information Society*, ITU, Geneva, 2006. 12 March 2009.

8. ITU, *Cyber security guide for developing countries*, Geneva, 2007. 5 Feb 2009. < http://www.itu.int/ITU >

9. The COMPUTER MISUSE ACT of 29th June 1990. http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1

10. Internet Usage and Population Statistics for Africa are for December 31, 2008.Retrieved May 1, 2009. <http://unstats.un.org/unsd/methods>.

11. Purdue University, Power Pool Development Group –ECOWAS, 2000, retrieved April 28 2009

12. Council of Europe action against cyber crime retrieved May 3, 2009. <http://www.coe.int/cybercrime>

13. Electronic Communications Transactions Act No.25 of 2002 http://pol.mcm.co.za/html/govdocs/legislation/2002/act25.html.21

14. Computer Security and Critical Information Infrastructure Protection Bill 2005, http://www.cybercrime.gov.ng/site/index.php?option=com_content&Itemid=56>. Retrieved March 10, 2009
    The Nigerian Communications Act 2003 http://www.ncc.gov.ng//

15. West African Power Pool (WAPP) agreements. Africa Renewal, Vol.18 #4 (January 2005) Retrieved April 23, 2009

16. IT Governance Institute. Retrieved April 15, 2009. http://www.isaca.org/AMTemplate.cfm