

# 1<sup>st</sup> Annual Conference of National Assembly Anti Money Laundering And Cyber Security Coalition

Combating Cyber Crimes in 21<sup>st</sup> Century

ENGR. E.C.A NDUKWE, FNSE, FNIM, OFR

EXECUTIVE VICE CHAIRMAN, NIGERIAN COMMUNICATIONS COMMISSION (NCC)

# Contents

- Background
- Overview
- Cyber Protection
- Challenges
- Conclusion

# Background

- Introduction
- Prevalence of cyber fraud globally
- The global nature of the crime – transcontinental transactions
- The penetration of cyber world

# General experience

- Everything relies on computers and the Internet now — communication (email, cellphones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on.

# Cyber connection

- Cyber - a popular prefix that connotes computer, its application and information systems.
- Virtually everything that can be computerized can be prefixed with Cyber.
- Cyber-law, Cyber-security, Cyberspace (Virtual Reality), Cybercafé (The Internet Business Centre), Cyber-bully, Cybernetics, Cyber Mall, Cyberburger Joint, Cybercast, Cybermediary, Cybernate, Cyberpunk,
- Cyberself, Cybersquatting, Cyber-stalker, Cyber-surfer, Cyber-terrorism, Cyber-bully, Cyber-crime, Cyber-thriller, Even In Some Local Languages Like Indian Cyber Dhaba (Equivalent Of Cybercafé), Cyber-woozling.

# General experience contd

- How much of your daily life relies on computers?
- How much of your personal information is stored either on your own computer or on someone else's system?
- When you hear IP-based system, it means cyber world, and this is where the new technologies and applications are leading us to.

# Global Prevalence of Cyber fraud

- Internet today is a vast fabric of computers – from supercomputers to handheld devices – and interconnected networks enabling high-speed communications, information access, advanced computation, business transactions, and automated processes all over the world as one large network.
- Because much of this infrastructure connects one way or another to the Internet, it embodies the Internet's original structural defective attributes of openness, inventiveness, and the assumption of good will.

# What are the risks

- Viruses erasing your information
- Someone breaking into your system reading and or altering your files
- Someone using your system to attack others
- Someone stealing your personal/ health/ insurance/ financial information and making unauthorised purchases or facilitating other unauthorised activities



# Penetration Risk

- There is no guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances
- A new survey of IT leaders shows that unstructured information such as email, instant messages (IM) and files is a root cause of security and business challenges.

# The global nature of the crime

- Because the internet is so accessible and contains a wealth of information, it has become a popular resource for communicating, for researching topics, and for finding information about people.
- It may seem less intimidating than actually interacting with other people because there is a sense of anonymity. However, you are not really anonymous when you are online.

# Personality Online

- People are typically wary of sharing personal information with strangers they meet on the street, but they may not hesitate to post that same information online. Once it is online, it can be accessed by a world of strangers, and you have no idea what they might do with that information.
- Personal information can easily be accessed.

# Overview

- Internet Structure
- Driven by IP – structure
- Different kinds of cyber frauds/crimes, identity theft, intrusions, threat
- The virtual nature of the cyberspace or anonymity of the source
- Technological advancement
- Internet Global network vs PSTN global network
- Transcontinental partnership and partnering

# Internet Structure/History

- The Internet was formed from the ARPAnet, a collection of military or defence-related computers operating with a high degree of trust in their users.
- This trust informed the design of the basic protocols of the Internet, which lacked strong authentication for users or for computers.
- In 1989, the ARPANET officially became the Internet and moved from a government research project to an operational network; by then it had grown to more than 100,000 computers.

# Internet Structure/History

- No one knew the Internet would hold valuable world information economy and resources today, and so no one thought to include protections against misuse of information.
- The result is that today there is widespread fraud on the Internet, both for direct financial gain and for indirect gains, such as theft of service or gains in access privileges.

# Internet Structure/History contd.

- Many early network protocols that now form part of the Internet infrastructure were designed without security in mind.
- Without a fundamentally secure infrastructure, network defense becomes more difficult.
- Furthermore, the Internet is an extremely dynamic environment, in terms of both topology and emerging technology.

# Internet Fraud

- The term *Internet fraud* is defined by the US Department of Justice Internet Fraud Center as "any type of fraud scheme that uses one or more components of the Internet—such as chat rooms, e-mail, message boards, or Web sites—to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme."
- This definition is consistent with, but not identical to, the definition in 18 PA C.S. Sec. 3933, where this activity is defined as a third-degree felony.
- This type of activity has affected individuals, corporations, and government agencies.



# 419 Operations

- Centralized counter-419 operations is the only way that viable statistics on 419 can be maintained. Decentralized counter-419 operations mean fragmented information and data.
- Everyone has a piece of the picture, but no one has the full picture.
- Something has to change.

# Internet Structure Contd.

- Transcontinental partnership and partnering
- An attacker does not have to be physically present to carry out the attack.
- Because of the inherent openness of the Internet and the original design of the protocols, Internet attacks in general are quick, easy, inexpensive, and may be hard to detect or trace.

# Driven by IP – Structure

- There is VoIP, Video over IP, IPTV, etc, and now Crime over IP, Fraud over IP, etc.
- IP drives the cyberspace. The other way of expressing this is by prefixing 'e' – e-business, e-transactions, e-ticket, e-medicine, e-governance, e-banking, etc.
- Today parlance: Crime over IP (CoIP), e-Crime
- The virtual nature of the cyberspace or anonymity of the source encourages e-crime

# Different kinds of cyber frauds

- Crimes, identity theft, intrusions, threat
- The major types of Internet fraud have been defined as 1) auction and retail schemes, 2) business opportunity or work-at-home schemes, 3) identity theft, 4) investment schemes, 5) credit card schemes, and 6) other schemes. Certainly, individuals have felt the brunt of many of these schemes, but corporations and government agencies have suffered as well.

# Fraud Variations

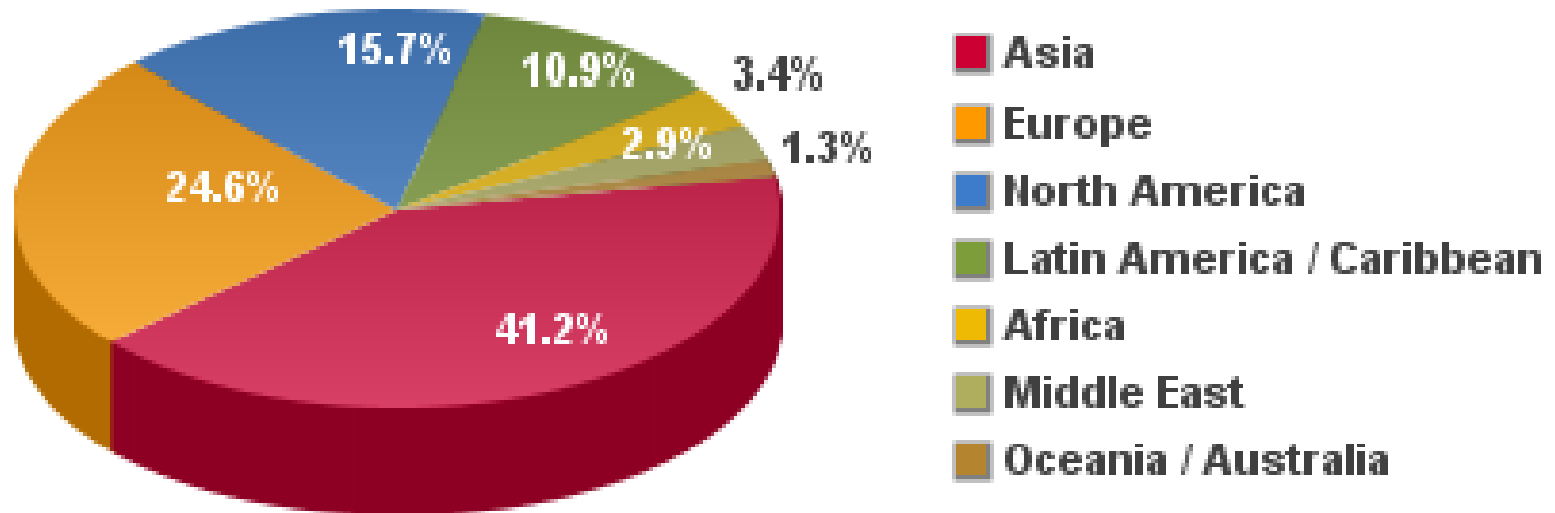
- The internet, cyber crime, and other variations of fraud statistics from many countries have separate categories: auction fraud, non-delivery, credit-debit card fraud, check fraud, confidence fraud, lottery fraud, Nigerian letter fraud, etc.

# Technological advancement

- Internet Global network vs PSTN global network
- IP driver of future networks.
- Convergence
- Product of digital technology
- Tremendous growth witnessed worldwide

# World Internet Statistics

## World Internet Users by World Regions



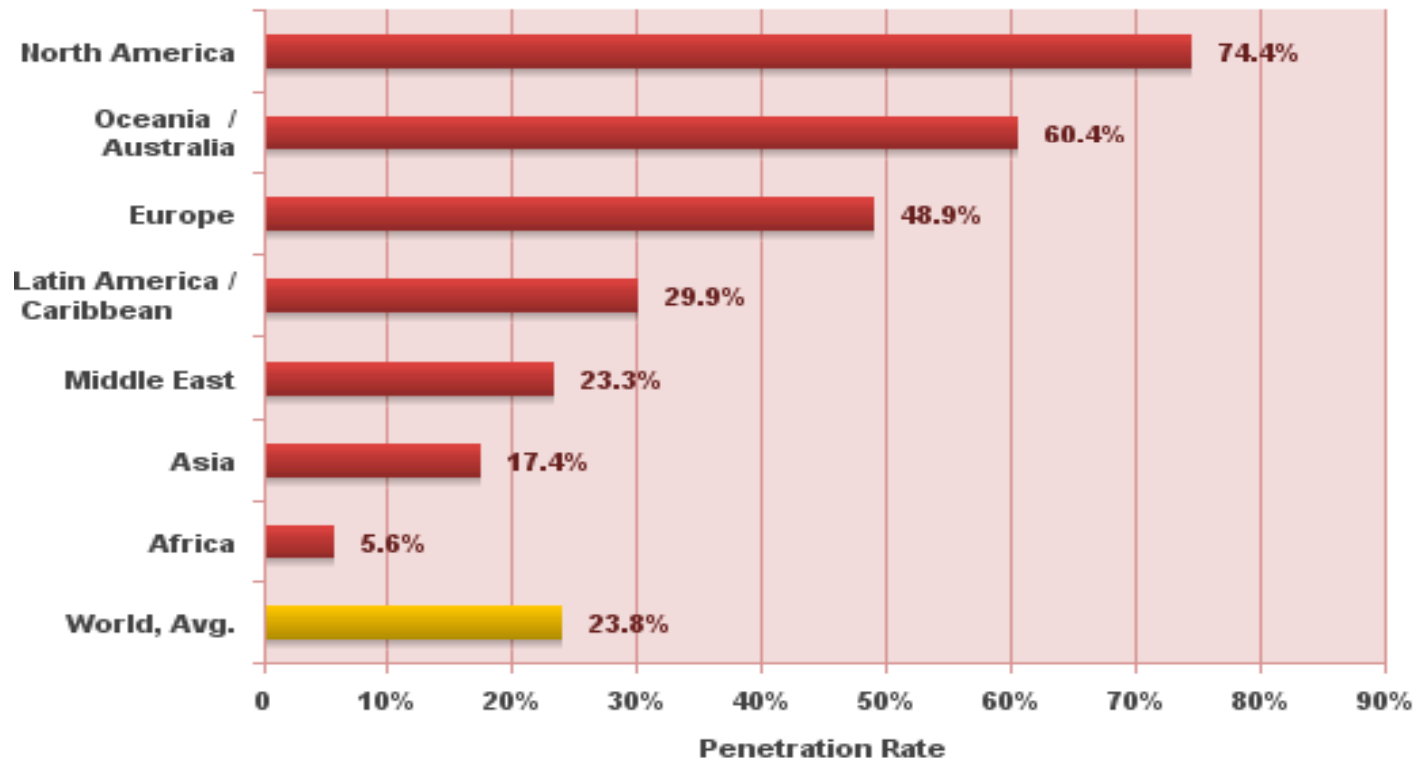
Source: Internet World Stats - [www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm)

1,596,270,108 Internet users for March 31, 2009

Copyright © 2009, Miniwatts Marketing Group

# World Internet Penetration

## World Internet Penetration Rates by Geographic Regions

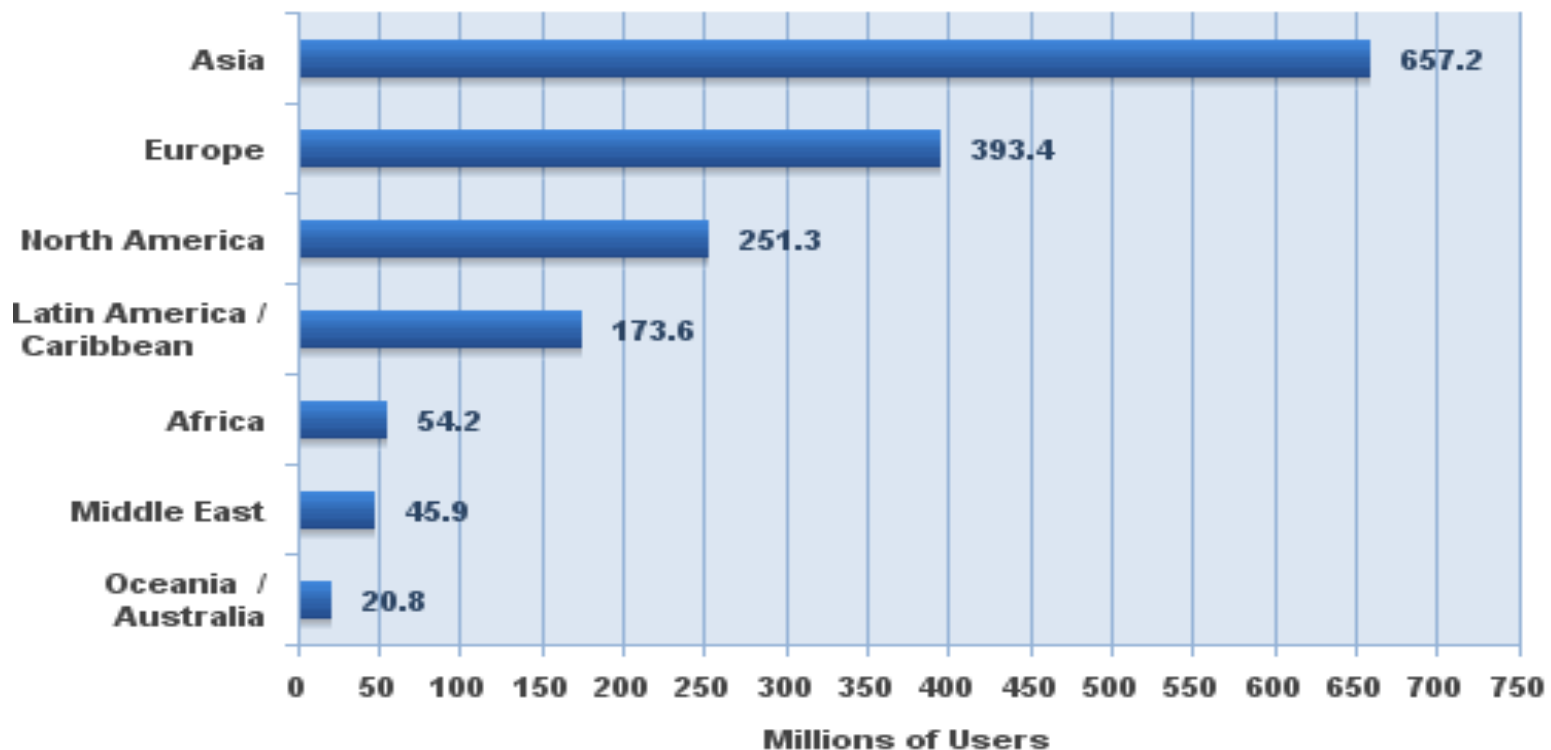


Source: Internet World Stats - [www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm)  
Penetration Rates are based on a world population of 6,710,029,070 and 1,596,270,108 estimated Internet users for March, 2009.  
Copyright © 2009, Miniwatts Marketing Group



# World Internet Usage

## Internet Users in the World by Geographic Regions



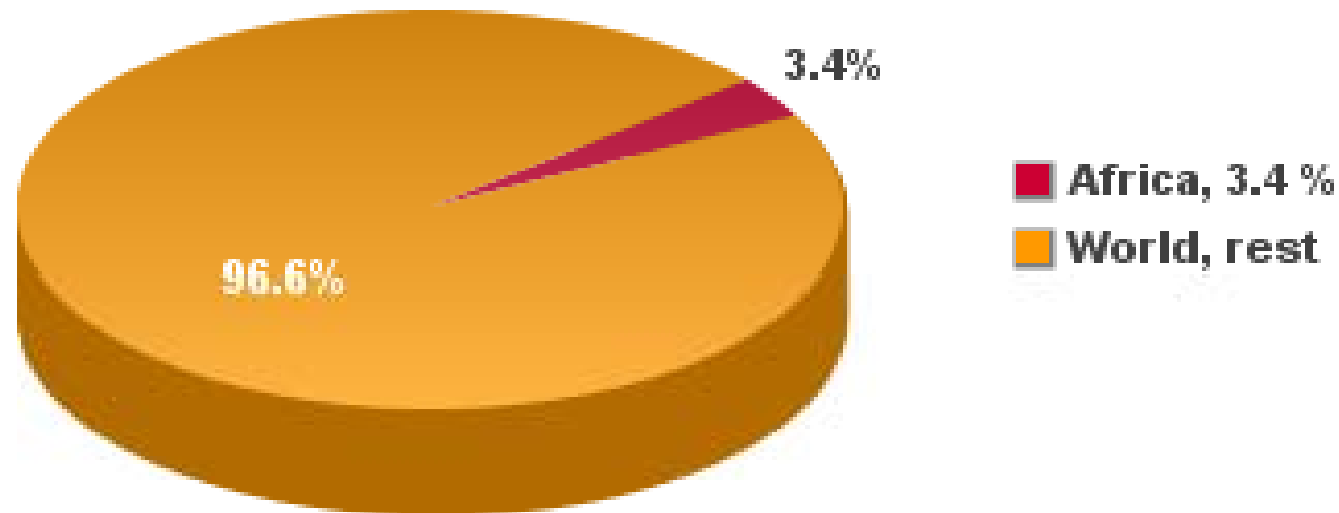
Source: Internet World Stats - [www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm)

Estimated Internet users are 1,596,270,108 for March 31, 2009

Copyright © 2009, Miniwatts Marketing Group

# Internet Usage in Africa

## User Internet Users in Africa Africa vs. World

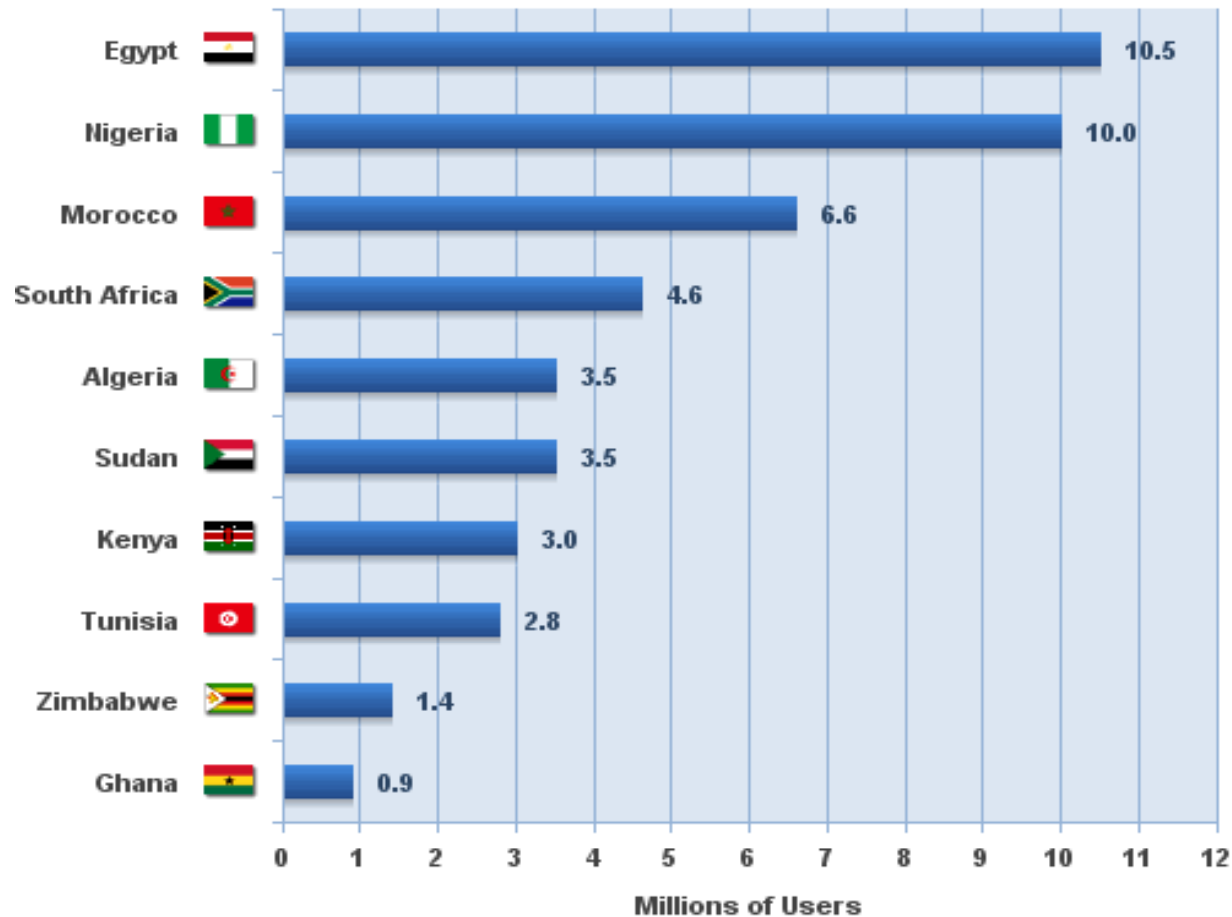


Source: Internet World Stats - [www.internetworldstats.com](http://www.internetworldstats.com)  
54,171,500 estimated Internet users in Africa for 2008  
Copyright © 2009, Miniwatts Marketing Group

# Internet Statistics

Africa

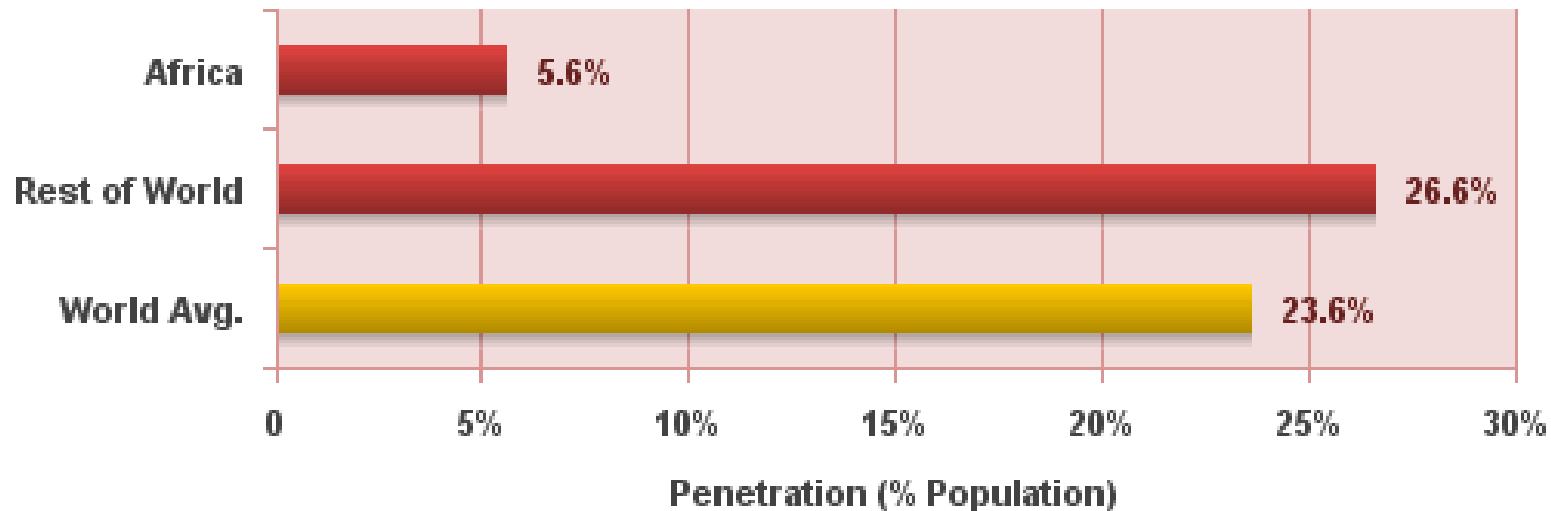
## Africa Top 10 Internet Countries



Source: Internet World Stats - [www.internetworldstats.com](http://www.internetworldstats.com) - Dec. 2008  
Copyright © 2009, Miniwatts Marketing Group

# World Internet Penetration

## Internet Penetration in Africa



Source: Internet World Stats - [www.internetworldstats.com](http://www.internetworldstats.com) - Dec. 2008

54,171,500 estimated Internet users in Africa for year-end 2008

Copyright © 2009, Miniwatts Marketing Group

# Nigeria's Deregulation

- Many Government owned companies were privatised.
- Serious growth in private sector
  - Banking
  - Telecoms
  - Stock exchange
  - Postal and courier services, etc.
- Telephone and broadband availability

# Infrastructure subject to CyberCrime

- Mail
- Fax
- Phone
- E-mail
- Chat rooms
- Dating web sites
- Matchmaking web sites
- Internet auction sites

# Infrastructure prone to CyberCrime

- Social and business networking sites
- Mobile phone SMS
- Internet phone
- Internet gaming (new)
- Personal introduction
- Call centre / boiler-room
- Door-to-door - in countries where an internet connection or sometimes phone or fax connections are not yet common circumstances.

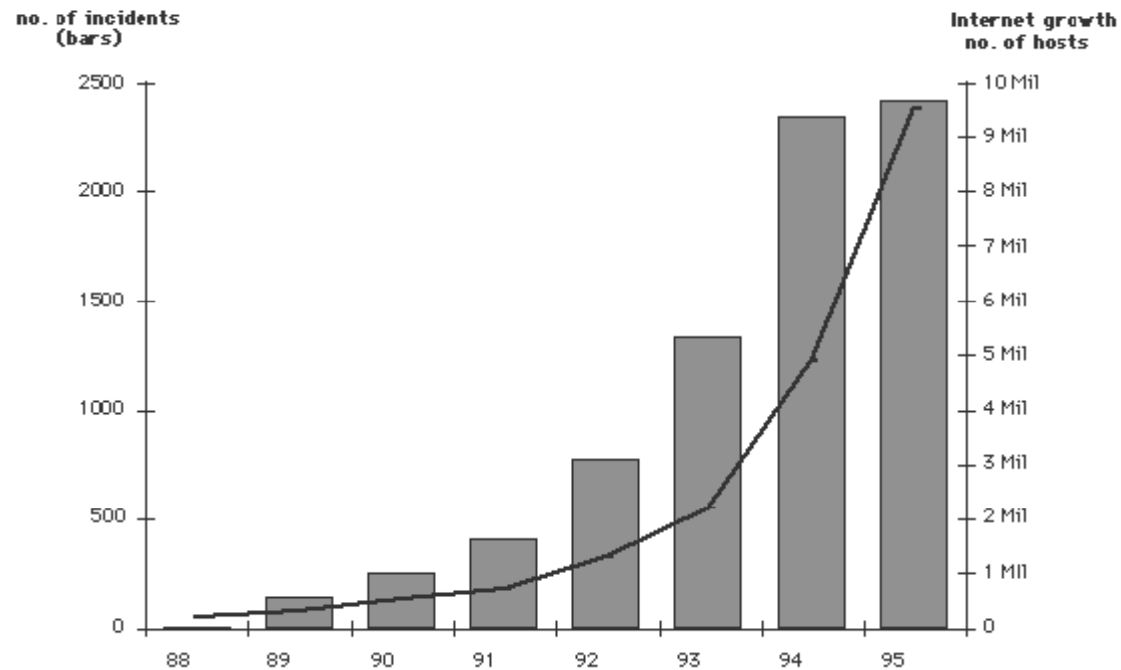
# Infrastructure prone to CyberCrime

- Social and business networking sites
- Mobile phone SMS
- Internet phone
- Internet gaming (new)
- Personal introduction
- Call centre / boiler-room
- Door-to-door - in countries where an internet connection or sometimes phone or fax
- connections are not yet common circumstances.

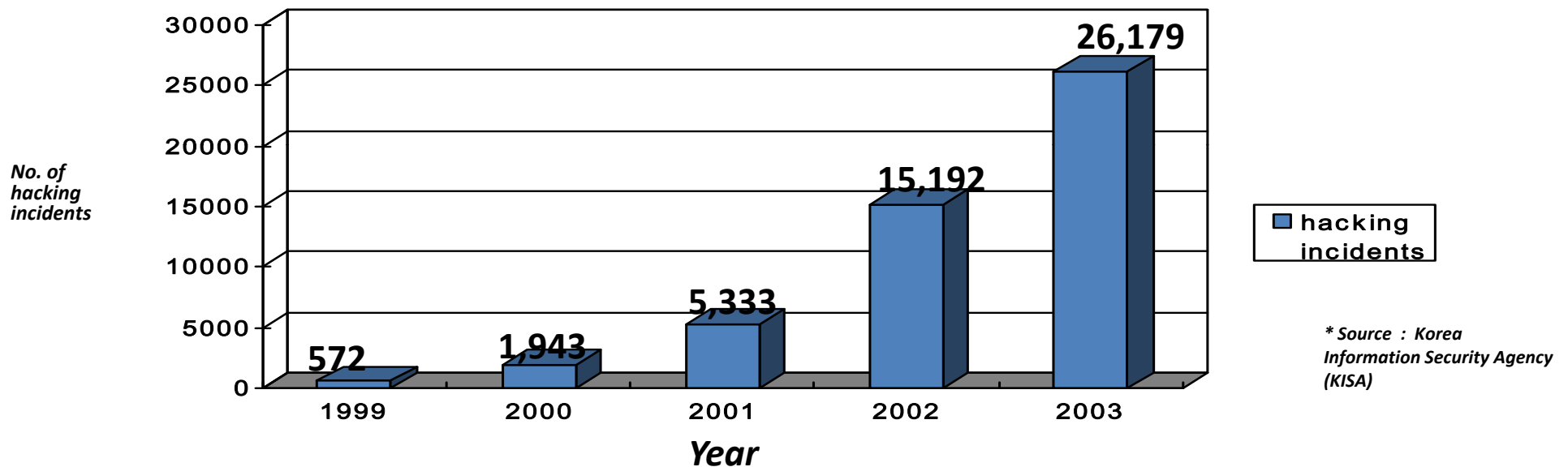


# Growth of Cyber Incidents

## Growth in Security Incidents



# Challenges & Threats to the Information Society



Hacking Incidents increased two or three-fold a year

Hacking and Virus become more sophisticated and malicious in a larger scale.

# Cyber Protection

- Regulation
- Presidential Advisory Committee on 419 activities in the Cyberspace (Internet)
- National Security Adviser
- Different Country experiences
- Need for united global approach (like the global meltdown)
- Policies and regulations
- Inter Departmental/ interagency cooperation
- Knowledgeable Approach

# Regulatory Development

- Three recognized distinct problem areas:
  - Critical Infrastructure Protection,
  - Intrusion Prevention and
  - Threat Assessment.
- The Internet infrastructure relies on primarily on the Border Gateway Protocol (BGP) and the Domain Name System (DNS).

# Different Approaches

- Presidential Advisory Committee on 419 activities in the Cyberspace (Internet)
- Different Country experiences
- Need for united global approach (like the global meltdown)
- Policies and regulations
- Inter Departmental/ inter-agency cooperation
- Knowledgeable Approach

# Presidential Advisory Committee

- President Olusegun Obasanjo in late 2003 or early 2004 setup PAC on cybercrimes.
- Several issues were identified including admission of cyber evidence as primary evidence
- Total dissection of the Cyber /ICT infrastructure
- Adequate training for the relevant monitoring team

# PAC

- Provide technical infrastructure to ensure true 24/7 availability.
- Equip and enable continuous training and maintenance of a dedicated cybercrime unit with law enforcement investigators and technical experts
- Create a Computer Security Incident Response Team
- Build a National Database on Computer Security Incidence and Response

# Challenges

- Regulation – issues on regulating a boundless resource cutting across several countries
- Sophistication- high tech application
- ICT – unprecedented development – more computers and applications get connected daily
- Internet Dynamism – ever evolving protocols
- Cybercriminals very knowledgeable
- Virtualness or anonymity of cyberspace- faceless
- Global Dimension – very huge
- Legal – Law on evidence- difficulty in accepting cyber evidence



# Conclusion

- There has to be a Master Plan detailing a strategic roadmap over a determined number of years that will guide the nation's efforts to protect the country against external and internal cyber threats. It should focus on further developing the country's cyber security capabilities while improving upon current efforts to prevent, detect and respond to cyber threats. It charts the directions and key strategies as well as programmes that will strengthen the resiliency and robustness of Nigeria's cyber infrastructure as well as raise the overall cyber security of our country.

# Conclusion

- Several discussions have been held over many years on the tremendous interconnectedness and interdependency among computer systems on the Internet. As a result, the security of each system on the Internet depends on the security of all other systems on the network. To address Internet fraud anywhere and other problems on the Internet, we must continue to work together. We must educate all users, take steps to protect information on Commonwealth computers, and invest in long-term solutions that benefit all.



## **Cyber Bully**

But what kind of Cyber Bully: identity thief,  
intruder, terrorist

Thank you.

**ENGR. E.C.A NDUKWE, FNSE, FNIM, OFR**

EXECUTIVE VICE CHAIRMAN, NIGERIAN COMMUNICATIONS COMMISSION (NCC)