A SPEECH

ON

UNIVERSAL BROADBAND ACCESS – NATIONAL SAFTY AND SECURITY IMPERATIVES

BY

EXECUTIVE VICE CHAIRAMAN /CEO
NIGERIAN COMMUNICATIONS COMMISSION
PROFESSOR UMAR GARBA DANBATTA, FNSE

26TH NATIONAL CONFERENCE & EXHIBITION

THEME:

INFORMATION TECHNOLOGY FOR NATIONAL SAFETY & SECURITY

JULY 19 - 21, 2016

May I stand on the existing protocol …

INTRODUCTION

The past two decades have been an unprecedented period for the development of information and communication technologies (ICTs) – with the advent of 'smarter phones' and rapid access to mobile devices the numerous benefits of ICTs has become within reach of practically everyone around the globe. By virtue of our regulatory posture within the sector, the NCC has been at the forefront of actualization of the National Broadband Plan 2013 – 2018 to ensure that everyone – irrespective of their circumstances or where they reside – have access to benefits of broadband.

Pervasive broadband access provides the platform for rapid socio-economic development by enhancing efficiency in business processes. In the area of public safety and national security, broadband provides opportunities for unique security applications and solutions. Although broadband also opens the cyberspace to various criminal activities, the benefits clearly outweigh the criminal tendencies.

SOCIO-ECONOMIC DEVELOPMENT, PUBLIC SAFETY AND BROADBAND PROVISION.

Public safety and national security are vital to Nigeria's prosperity. But most seldom seen only from the perspective of the military and paramilitary intervention. It is even less obvious that basic safety systems such as the pervasive CCTV surveillance in homes, offices, streets and public areas depend on broadband to record data / information and transmit them to remote storage locations for analysis. Broadband provides a platform for efficient and reliable communication before, during, and in the aftermath of disaster emergencies. Broadband in developed countries is enabling new ways of achieving public safety - including new ways of calling for help and receiving prompt emergency response.

Broadband networks are essential in the gathering and transmission of data for monitoring extreme weather conditions to anticipate natural disasters such as flood, famine, or the threat from extraordinary weather event such as Hurricanes, Typhoons, Tsunamis etc.

During a natural disaster, such as Nigeria's flood disaster or gas explosion, the availability of high-speed networks would make all the difference in terms of emergency response coordination. Under such circumstance, someone with a Smartphone in his hand can relay vital information to aid proactive planning by relief agencies and other responders, including news gathering and dissemination.

Broadband has become a key priority of the 21st Century, and its life-changing capability for enabling socio-economic growth makes it an essential tool for empowering people, creating environment that nurtures technology and service innovations and triggering positive change in general business processes. It is believed that increased adoption and use of broadband in the next decade and beyond will be driven by the extent to which broadband-supported services and applications are not only made available to, but are also relevant and affordable for consumers. And while the benefits of broadband-enabled future are manifest, the broadband revolution has also raised new issues and challenges – cybercrimes.

The Commission believes that expanding broadband penetration / access throughout the country is key to accelerating progress towards harnessing its full benefits - rapid socio-economic development. It is therefore the intention of the Commission to maintain a cyber-environment that encourages economic prosperity, certainty of delivery and transaction execution while promoting efficiency, innovation, safety, security, privacy and business confidentiality. It is also in this light that the passing into law of the Cybercrimes ACT of 2015 by the Federal Government should be commended.

The government has also appropriately put in place a National Cybersecurity Policy and Strategy to provide an overall framework for combating cybercrimes. The Federal Government of Nigeria is establishing Emergency Call Centers in all the 36 states of the federation and the FCT with a three-digit emergency code number, known as E112. When people dial 112 the call goes to the nearest Emergency Call Centre. Broadband makes the E112 Emergency system more capable and efficient by providing more voice channels for the service, including Voice over Internet Protocol (VoIP).

IMPROVING NATIONAL SECURITY AND PROTECTING CRITICAL INFRASTRUCTURE THROUGH BROADBAND IMPLIMENTATION.

Network Service Providers have continually experienced attacks on critical Internet infrastructures. A variety of local and non-local entities have demonstrated the ability to steal, alter or destroy data and to manipulate or control systems designed to ensure the functioning of portions of critical infrastructure. Additional safeguards are necessary to protect our nation’s communications infrastructure from cyber-attacks. Such safeguards could promote confidence in the safety and reliability of broadband communications and spur unhindered adoption.

Existing laws would therefore need to be upgraded to cover new areas such as electronic transactions, e-commerce and cyber security etc. NCC realizes that every modern nation depends on reliable and functional critical infrastructure to guarantee national and economic security. While the Cybercrimes ACT 2015 has some provision for the protection of critical infrastructure, a holistic approach to Critical National Infrastructure (CNI) protection needs to be adopted.

The NCC is promoting seamless interconnectivity through a universal broadband penetration drive aimed at attaining a robust National Fibre Optic Backbone Infrastructure, by providing quality regulatory interventions in terms of industry ethics, level playing ground, fair and transparent competition.

The broadband policy allows prospective companies, known as Broadband Infrastructure Companies (INFRACOS), to bid for licenses on regional basis – the Commission has already started licensing INFRACOS since last year.

It also encourage/enforce last mile infrastructure sharing regime that enables new entrants to spring up and thrive in the industry.

With high broadband penetration rate, a considerable surge in internet access and utilization is envisaged, including applications in the area of Internet of Things (IoT). This will surely open up new frontiers for our national security operatives to come up with customised and unique security applications /solutions to effectively combat modern cyber threats, while at the same time enhancing their collaboration with other similar international agencies.

CONCLUSION.

It is imperative that a clear roadmap for securing vital information and communications infrastructure / networks be developed.Such framework should be robust and effective enough to covercritical infrastructure in the areas of public safety and communications.It should also address cybersecurity holistically by identifying the most critical threats to communications infrastructure and its end users. The roadmap could establish a yearly plan, including milestones, to mitigate these threats. The recently inaugurated National Cybersecurity Advisory Council (CAC), which is a provision of the Cybercrimes ACT of 2015, is saddled with the responsibility of advising the government on general implementation strategies.

Security is everybody's' business, protecting against information security risks is part of protecting privacy. Collaboration between Ministries, Departments and Agencies (MDAs) and relevant stakeholders from the public and private sectors to help protect against increasing cybersecurity risks, is therefore imperative.

Cybersecurity is a shared responsibility, and each of us has a role to play in making the cyberspace safer, more secure and resilient. While the vast majority of the nation's cyber infrastructure resides in private hands, the risks to national and economic security associated with the compromise or failure of these assets means that their protection requires concerted public-private partnership initiatives.

Thank you.

GENERAL REFERENCES.

1. Nigeria's National Broadband Plan 2013 – 2018
2. ncc.gov.ng
3. Broadband.gov
4. www.cert.gov.ng
    i. National Cybersecurity Policy and Strategy
    ii. Cybercrime ACT, 2015
5. Fcc.gov
6. http://thenationonlineng.net/broadband-plan-without-support/
7. http://broadbandtoolkit.org/
8. http://www.broadbandcommission.org/

MEASURES CURRENT BEING TAKEN BY NCC

The NCC is in the process of setting up a sector based CSIRT that will work hand in hand with, and support the ngCERT, in tackling issues that relate to the telecommunications industry.

A digital forensics laboratory is also being established by the Commission.

With information provided by relevant sector CERTs - CERRT, NCC CSIRT, etc. and the ngCERT, Service Providers should have capabilities that will allow them more effectively identify and analyze malicious activity transiting through their networks.

The Commission is also collaborating with the International Telecommunications Union (ITU) to establish (here in Nigeria) a Regional Cybersecurity Center (RCC) for Africa.

The center will provide support in the area of technical manpower training, information sharing and other collaborative roles with local CERTs in the African region.

The Commonwealth Telecommunications Organization (CTO), which is currently chaired by the NCC, is playing a key role in ensuring that all its member states take great strides in achieving international collaboration in the area of cybersecurity.