# ADDRESSING THE VULNERABILITY OF CRITICAL ICT INFRASTRUCTURE

## Presentation at the NIGF 2013

by

**Ernest Ndukwe, OFR**
**Chairman**
**Openmedia Communications Ltd**

18th June, 2013

# CRITICAL INFRASTRUCTURE

## According to Wikipedia

“**Critical infrastructure** is a term used by governments to describe assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for:[1]

**Electricity** Generation, Transmission And Distribution; **Gas** Production, Transport And Distribution; **Oil And Oil Products** Production, Transport And Distribution; **Telecommunications**; **Water Supply** (Drinking Water, Waste Water/Sewage, Stemming Of Surface Water (E.G. Dikes And Sluices)); **Agriculture**, Food Production And Distribution; **Heating** (E.G. Natural Gas, Fuel Oil, District Heating); **Public Health** (Hospitals, Ambulances); **Transportation Systems** (Fuel Supply, Railway Network, Airports, Harbours, Inland Shipping) ; **Financial Services** (Banking, Clearing); **Security Services** (Police, Military)”

# CRITICAL ICT INFRASTRUCTURE

The term **critical ICT Infrastructure for Nigeria** in the new Nigerian National Broadband plan is defined as:

ICT networks and systems that are crucial to the Federal Republic of Nigeria to the extent that the damage, destruction or ineffectiveness of such networks and systems, whether physical or virtual, would have adverse impact on national security, economic wellbeing, public safety, food security or any combination thereof.

# THE BENEFITS OF ICTs

ICT networks are making it possible for African nations to participate in the world economy in ways that simply were not possible in the past

ICTs including Broadband constitute essential infrastructure of the Digital Economy of today.

No modern economy can be sustained today without adequate and pervasive ICT infrastructure

# ICT dependencies across other critical infrastructures

- Information and communication technology (ICT) pervades heavily into all areas of society, industry and government. It acts as a vital cross-sector dependency linkage between critical infrastructures.
- In fact, infrastructures such as telecommunications, energy and transportation are becoming increasingly dependent on each other through the increased use of  ICT.
- Therefore, the consequences of disturbances of  underlying ICT-networks may result in disastrous cascading effects on other sectors of the economy and consequently the nation’s socio-economic wellbeing

# Vulnerability

- Every modern nation depends on the reliable functioning of its critical infrastructure especially its ICT networks and systems.
- Increased dependencies on ICT infrastructure by other sectors could lead to increased vulnerability of the economy as a whole.
- A further case for critical infrastructure protection.

# Attacks on ICT Infrastructure

There are two broad categories of attacks that could adversely affect the nation's Critical ICT infrastructure, namely:

- Cyber attacks and
- Physical attacks (vandalism, sabotage and theft)

# CYBERSECURITY

# Cybersecurity

The adoption and usage of internet and broadband by everyone are essential prerequisites of the digital economy of the 21st century

However all over the world, cyber threats continue to grow and constitute major national security vulnerability points.

It must therefore be the intention of every government in the digital age to maintain a cyber environment that encourages economic prosperity while promoting business efficiency, innovation, safety, security and confidentiality

# Cybersecurity

It is therefore essential that government urgently enacts **comprehensive Cybersecurity Laws** to address the liability and criminal risks that may originate from inappropriate use of internet infrastructure

# Cybersecurity

In addressing vulnerability, there will also be need for:

- International coordination
- Exchange of Intelligence
- Training and Manpower  development of subject matter experts
- Ensuring that operators of Critical Infrastructure protect their systems from harm

# PHYSICAL ATTACKS

# Physical Attacks

ICT infrastructures have recently been subjected to physical damages all over the country:

✓Cut to submarine fibre cables

✓Cut to intra-city and interstate fibre cables

✓Criminal disruption of services

✓Cable theft

✓Terrorist Attacks

# Vulnerability

- Perhaps the greatest vulnerability comes from lack of awareness and acceptance of the risk posed to the nation’s infrastructure and economic wellbeing by these threats or attacks.
- The new broadband plan requires that ICT infrastructure be declared Critical National Infrastructure
- This is a necessary first step in mitigating the risks

# Other Physical Issues

Vulnerability can also occur from:

- Non-timely renewal of technologies and systems
- General failures in technology, systems or processes
- Usage that far exceed original design specifications
- Too much centralisation of infrastructure leading a possible single point of failure

# Final Thoughts

- It does not really matter whether critical infrastructure is lost or disrupted due to terrorism, bad planning or deterioration.
- What is essential is to develop a long-term infrastructure vulnerability mitigation strategy with close collaboration between government and the  operators, in order to address infrastructure design, protection and  upgrades
- This issue needs to rise to the level of a national agenda and given high priority status

# Thank You