# Developing Economies & Cybersecurity: Securing the "WEAKEST LINK" of the Information Society

**Basil Udotai, Esq.**

Coordinator,

Nigerian Cybercrime Working Group (NCWG)

**WSIS ITU Thematic Meeting on Cybersecurity**

Geneva, Switzerland

June 28 – July 1, 2005

# Preliminary Comments

- **Developmental Paradox of Cybersecurity**: promoting ICT adaptation and internet penetration, while at the same time warning of the dangers of cybersecurity!
- **Funding for ICT Projects:** by development partners who are careful not to talk about cybersecurity – Nigeria's IFEMIS Project (EU); NFIU (the World Bank) is the once popular concept of "sustainable development" totally dead and buried?
- **First things First:** Life would be so much easier if the requirements for cybersecurity were incorporated into the conditions of these projects!
- **How about Nigeria and 419?:** Do you really think we enjoy this?
- **ECOWAS September 2005:** Meeting of ECOWAS Attorneys General on Cybercrime; Abuja September 22 – 24, 2005

# The Weakest Link Phenomenon

- “While the biggest spammers in the World are located in the United States and Russia, their operations are hosted by ISPs in China” - **Steve Linford, CEO, Spamhaus Project**
- “The fight against cybercrime either is a global one or it makes no sense” – **Guy DE VEL, Director General Legal Affairs, Council of Europe**
- “When it comes to combating cybercrime across international boundaries, the chain is truly only as strong as its weakest link” – **John Malcom, Deputy Assistant Attorney General, Senate Judiciary Committee, February 24, 2004**

# Who is the Weakest Link?

- If Cybersecurity is really about "technology, processes and people" then the countries least prepared in terms of technology, processes, skill/awareness (people) constitute the weakest link on chain of the Global Information System;
- Where are these countries?
- Developing Economies, especially those south of the Sahara.
- Since the Internet is truly global and inherently insecure, these weakest links have and will continue to pose the greatest risks to Internet security;
- Developing economies, "You are the Weakest Link, Goodbye"
- Wouldn't that just be nice? But, no can't do - design of the Internet itself males this impossible;
- "Fear factor:" We are truly in this together

# Why is the weakest link phenomenon important?

- Determines cybersecurity forum shopping – the act of originating cyber attacks from least regulated or most permissive jurisdictions or using those countries as pass through hubs to transmit cyber attacks;
- China and Russia (SPAM) typify the trend of cybersecurity forum shopping - should solution be found for China and Russia, Spammers/hackers would migrate to other favorable destinations;
- Informs the new basis for cooperation, should the World be interested in fostering a TRULY global culture of cybersecurity;
- Connectivity is the new basis upon which cybersecurity assistance should be predicated in the Information Society, not the traditional basis of erstwhile global cooperation and assistance - Proximity; Culture & Tradition – (Language, religion, etc); History; Strategic Economic Interest;
- Unfortunately global cybercrime efforts so far have tended to follow these traditional models of cooperation

# Cybersecurity ….. not Rwanda

- The Neighborhood Principle popular in the Law of Torts – "anyone likely to be affected by my action is my neighbor" – acquire greater meaning in the Internet than traditional torts law: the Internet makes everyone your next door neighbor and every country a border nation;
- SPAM: United States/China/Russia;
- Terrorism (9/11): United States/Turkey/Nigeria;
- Malicious publication: Australia/USA;
- "I Love You": The Philippines/several countries – connectivity determined harm, not physical proximity;
- Needless to say that the notion of their problem, not our problem (Rwanda) which tend to mark most international relationships building and global cooperation; will FAIL if applied to address Internet security

# Some Realities

- As a Group, how much do Developing Economies care about cybersecurity? Not very much – but don't take my word for it. Ask Tanzania, Zambia, Uganda, Lesotho, Ethiopia, Mauritius – mostly there are no laws, but where there are laws, enforcement is lacking
- Can we tell what's going on in our networks: whether stored or real time? Terrorist arrested in Pakistan confessed to using servers in Turkey and Nigeria to disseminate coded messages to other operatives around the World!
- Is it a crime? Where is the evidence? Who collected it? Would the courts take the case? Would the accused be convicted?

- Only one legal consequence await Cyber attackers and Spammers in most developing countries:

**NOTHING!!**

# Redefining global cooperation

- The Internet, more than anything else before now, has the greatest potential for redefining global cooperation;
- Realities of forum shopping; little or no incentive for security in developing economies; connectivity not proximity determining our neighbor;
- Evolving a truly global culture of cybersecurity means assisting developing economies adopt the “technology, processes and people” of cybersecurity;
- Accomplishing global cybersecurity is  not only essential for the survival of the new Information Society, but it becomes a matter of strategic economic interest for advanced economies;
- May force a redefining of global cooperation

# What manner of assistance?

- Whatever is necessary to bring about the “technology, processes and people” of cybersecurity in the developing economies;
- Developing economies may not ask for help – incentive for cybersecurity;
- Developed economies may have to initiate the assistance;
- While all manner of assistance should be exploited, Political assistance may be the most productive;
- National Cybersecurity framework could be made condition for debt relief and other development assistance; return of looted funds uncovered in advanced countries; accession into the EU or even the WTO;
- High profile politicians and heads of major global organizations should include the need for national cybersecurity initiative in their speeches as they visit developing countries; the US and the World Bank missed good opportunities in Nigeria earlier this year

# ITU

- ITU should be at the forefront of the effort to evolve a truly secure global information system;
- Should consider establishing a Unit to promote cybersecurity in the developing economies and harness development assistance initiatives of the advanced economies;
- Such a Unit would be responsible for organizing regular meetings amongst developing economies; monitor progress made at national levels, document cybersecurity measures adopted by developing economies and coordinate experience sharing both on a peer-to-peer basis amongst developing countries and between their advanced counterparts;
- The Unit might come to posses the much needed intelligence on cybersecurity initiatives in developing economies, upon which further development programs may depend.

# 419

- **Government not doing enough? Deliberate inaction? Massive capital flow by default?**
- **Matter of Public International Law; national criminal law can only ideally target domestic harm; Extraterritoriality as basis of national law - hinges on foreign acts occasioning substantial domestic harm;**
- **Strong moral element requiring foreign legal intervention;**
- **419 activities gone global - Verisign**
- **Remedying extraterritorial injury ONLY possible with local law – done that already – Advance Fee fraud Act, EFCC Act, Money Laundering Laws, etc**
- **Old/New: traditional law and enforcement mechanisms employed to tackle what has become largely a tech problem;**
- **Hundreds arrested, billions confiscated; hundreds of prosecution; but not a single conviction on Internet 419**

# Other Challenges

- Developmental Paradox of Cybersecurity – “Prophet of Doom: make up your mind; will ICT make us or break us?” – actual question on national TV!
- We are not there yet? Build roads and put food on the table; meanwhile private sector, government and citizens are adopting ICT and becoming increasingly reliant;
- Unique criminal law culture of Nigeria – statute creates Agency, criminalize certain conducts, authorize that Agency only to enforce those conducts under the same law creating the Agency – EFCC, NDLEA, ICPC, etc;
- Definition of institutional competence and overlap of responsibilities;
- Original conception for cybercrime – central agency for the enforcement of all cybercrimes – discussion with stakeholders necessitated change in approach;
- Decision makers have scant experience in ICT and are unable to support cybersecurity initiatives;
- Deliberate Misinformation for non-security motives;
- Battle to take credit for solution

# The National Cybersecurity Initiative (NCI)

- Being implemented by the Nigerian Cybercrime Working Group (NCWG);
- It main aim is to fashion appropriate Legal and Institutional framework for:
- a. Securing Computer Systems and Networks; and
- b. Protecting Critical infrastructure in Nigeria

# The Nigerian Cybercrime Project Background

- Presidential Committee on Cybercrime
- Report recommended creation of a legal and institutional framework for cybercrime in Nigeria
- Enhance capacity of law enforcement institutions to tackle enforcement institution
- Create the Nigerian Cybercrime Working Group (NCWG) as an inter-agency body of law enforcement, intelligence, security and ICT institutions, plus private sector
- Propose a Draft law, the Computer Security and Critical Infrastructure Protection Act, as the operative legal instrument for cybersecurity in Nigeria

# The Nigerian Cybercrime Working Group (NCWG)

- an Inter-Agency body made up of all key law enforcement, security, intelligence and ICT Agencies of government, plus major private organizations in the ICT sector; including Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF); the National Security Adviser (NSA), the Nigerian Communications Commission (NCC); Department of State Services (DSS); National Intelligence Agency (NIA); Nigeria Computer Society (NCS); Nigeria Internet Group (NIG); Internet Services Providers' Association of Nigeria (ISPAN); National Information Technology Development Agency (NITDA), and Individual citizen representing public interest. 2 Chairman and one Coordinator.

- ToR include public enlightenment, building institutional consensus amongst existing Agencies, providing technical assistance to the National Assembly on Cybercrime and the Draft act; laying the groundwork for the Cybercrime Agency, etc.

- Commencement of Global cybercrime enforcement relations – CCIPS (USA), NHTCC (UK), NPA (SA)

# The Draft Bill: Computer Security and Critical Infrastructure Protection Act

- Substantive – criminalize conducts against ICT systems, using ICT systems and targeting critical infrastructures
- Procedure – judicial procedures for investigation and prosecution
- Data retention and interception;
- Constructively amend all traditional Intellectual Property laws and the Evidence Act
- Vests enforcement responsibilities on all Law Enforcement Agencies in Nigeria
- Framework for cooperation with international law enforcement organizations Worldwide

# Nigeria will pursue this process

- Constitutional prerogative of government to enforce law: sophistication of crime or high-tech nature of media not excuse for inaction;
- Success in ICT in Nigeria = Fastest growing market in telecoms – ITU, more than $12 billion FDI in just 4 yrs (NCC); phone lines grown from 350,000 in 2000 to 14million in May 2005;
- Increasing dependent on ICT: personal, business and government;
- Information infrastructure fast becoming critical to Nigeria’s economic and social well being;
- Damage would have expansive effect
- ICT is a “test case” for other FDI

# THANK YOU

CONTACT:

**Nigerian Cybercrime Working Group (NCWG)**
**Office of the National Security Adviser**
**Three Arms Zone**
**Aso Rock Villa**
**Abuja**
**Office+234-222-3000;**
**Mobile +234-803-306-6004**
**b.udotai@cybercrime.gov.ng**
**www.cybercrime.gov.ng**