CYBERCRIME LEGISLATION DEVELOPMENT IN NIGERIA – AN UPDATE

Octopus Conference, Strasbourg
06 June, 2012

T.GEORGE-MARIA TYENDEZWA
Head, Computer Crime Prosecution Unit,
Federal Ministry of Justice,
Abuja, Nigeria

Introduction

- Several Draft Cybercrime Bills had been pending in the National Assembly since 2006
- ONSA Committee in November, 2011, produced the harmonized ***Cybersecurity Bill, 2011,*** **for transmission to the National Assembly for passage as an executive bill.**

Harmonized Cybersecurity Bill, 2011

- **Part I – General Objectives**
- Part 1 deals with the general objectives, the scope of the Bill and its application.
- The objects and scope of this Act are to –
- provide an effective, unified and comprehensive legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
- Enhance cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, Intellectual property and privacy rights;
- The provisions of this Act shall be enforced by law enforcement agencies in Nigeria to the extent of an agency's statutory powers in relation to similar offences.

Harmonized Cybersecurity Bill 2011

- **Part II – Offences & Penalties**
- This Part (Sections 2 to 18) criminalizes specific computer and computer – related offences, which include: Unlawful access to a computer; Unauthorized disclosure of access code; Data forgery; Computer fraud; System interference; Misuse of devices; Denial of service; Identity theft and impersonation; Child Pornography; Records Retention and Preservation; Unlawful Interception; Cybersquatting; Cyber-terrorism; Failure of Service Providers to Perform certain Duties; Racist and xenophobic Offences; Attempt, conspiracy and abetment; and Corporate Liability.

Harmonized Cybersecurity Bill 2011

- **Part III – Critical Information Infrastructure Protection**
- Part III provides for the security and protection of critical information infrastructure. It further provides for the audit and inspection of critical information infrastructure and punishment for offences against critical information infrastructure.
- **Part IV – Search, Arrest and Prosecution**
- Part IV deals with issues such as jurisdiction, powers of search and arrest, obstruction of law enforcement officers, prosecution, forfeiture of assets, compounding of offences; payment of compensation; and the power to make regulations.

Harmonized Cybersecurity Bill 2011

- **Part V: International Cooperation**
- Cybercrime and cybersecurity issues are not restricted by geographical boundaries and legal jurisdictions but can only be checked through international cooperation which is covered in Sections 29 to 34 of the Bill. The issues covered include: Extradition; Mutual Assistance Requests; Expedited preservation of data, Evidence Pursuant to a Request; and Form of Requests

- **Part VI: Miscellaneous**
- Part VI deals with issues of a general character such as Directives of a general character; Regulations and the Interpretation.
- The above provisions of the draft Cybersecurity Bill, 2011 have met the milestones required of legislation on cybercrime, even when reviewed or compared against international instruments and standards, such as the Council of Europe's *Budapest Convention,* 2001[3] and the *ITU Toolkit on Cybersecurity Legislation.*

Progress Made - Slowly

- The harmonized ***Cybersecurity Bill, 2011,*** *has undergone review by various stakeholders with the aim of* ensuring broader buy-in & a operational partnership with all stakeholders.

- The harmonized ***Cybersecurity Bill, 2011,*** *is* currently being corrected as reviewed to create the final draft that will go to the legislature for passage into law, by a ministerial committee set up by the Honourable Attorney General of the Federation on 23 April, 2012.

Challenges…

- General lack of awareness among LEAs, legal practitioners, judges, etc…
- Lack of LEA capability/capacity - Not enough officers trained and equipped to act as first responders
- Contamination of crime scene/destruction of electronic evidence ab initio due to ignorance
- Lack of forensics laboratory for investigation & evidence analysis/case preparation
- No electronic evidence handling/management capacity in the courts,
- Lack of training & resources for prosecutors, LEAs and judicial officers…

CONCLUSION

The good news is that the Nigerian government notes the imperative for domestic legislation to fight cybercrime and is committed to putting in place the requisite legal and institutional framework to ensure Nigeria can derive meaningful economic and social value from a vibrant, resilient and secure online environment and make sure that we can co-operate with other countries to on cross-border law enforcement and deny safe havens to cyber criminals.

Questions?

THANK YOU.

T.G. George-Maria Tyendezwa,
Head, Computer Crime Prosecution Unit,
Federal Ministry of Justice,
71B, Shehu Shagari Way, Maitama , Abuja
M: +234 803 322 0559
E: george.tyendezwa@fmj.gov.ng
W: www.fmj.gov.gov/ccpu