LEGISLATION ON CYBERCRIME IN NIGERIA: IMPERATIVES AND CHALLENGES

T.G. George-Maria Tyendezwa,

Head, Computer Crime Prosecution Unit,

Federal Ministry of Justice,

OUTLINE

- Interconnected world
- The Nigerian situation
- Crimes in an interconnected world
- The imperative for Nigeria
- Legislation and institutional framework
- Challenges
- Recommendations
- Conclusion

Interconnected world

- High speed communications and convergence
- Social Media and Interactions (Facebook/Twitter)
- 5 Billion interconnected devices
- $8 Trillion in e-commerce transactions
- Migration of businesses to online environment
- Government services have now gone online

The Nigerian Situation

- E-government services
- Payment platform for e-Commerce
- ATM Machines
- Electronic Activities of the NSE
- Cashless Lagos and soon Nigeria
- Electronic Identification system

Crimes in an Interconnected World

- All crimes imaginable offline can be achieved with the use of computer networks as a tool
- Threats to lives and properties
- Disruption of critical services
- Terrorism and economic sabotage
- Propaganda
- Theft of information(identity & credit card theft)

The Imperatives for Nigeria

- Establishment of Legal and Regulatory Framework
- Establishment of Institutional Framework for coordination of implementation;
- Standards and Regulations;
- Capacity Building
- Compliance & Enforcement;
- Emergency Response & Readiness;
- Public enlightenment
- International Cooperation

Legislation and Institutional Framework

- Several Draft Bills pending in the National Assembly
- NSA's Committee on Cybersecurity Bill 2011
- - General Objectives
- - Offences and Penalties
- - Critical Information Infrastructure Protection
- - Search Arrest and Prosecutions
- - International Cooperation
- - Miscellaneous

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.

Harmonized Cybersecurity Bill 2011

- **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

Harmonized Cybersecurity Bill 2011

- **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.*

Challenges

- Turf battles (supremacy disagreements) among law enforcement, intelligence and security agencies;
- Lack of understanding of the dire consequences of not criminalising conduct that amounts to cybercrime or the serious dangers, economic loss and national security vulnerability that flows from the lack of adequate cybersecurity framework, on the part of our lawmakers;
- The absence of a knowledgeable and committed champion at the highest policy levels to sustain the drive for the passage of the Bill, while emphasising the peril of not doing so.
- Lack of integration of public – private sector stakeholders in the process, due largely to distrust of government by the private sector, as well as sectored infighting;
- Insufficient sustained lobbying of the lawmakers by the sponsors of the various previous pending Bills.

Recommendations

- Enactment of substantive laws to criminalize malevolent activities on the internet
- Capacity building
- Cooperation between actors (Private or Public)
- Establishment of Institutional framework for coordinating cybersecurity efforts
- Enactment of related Bills to strengthen the cybersecurity framework

Conclusion

Completion of the legislative process and establishment of institutional framework should be considered a matter of urgency

A state of Emergency should be declared in this area until the recommendations in this paper are implemented

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