FEDERAL REPUBLIC OF NIGERIA

VIEWS ON THE SCOPE, OBJECTIVES, AND STRUCTURE (ELEMENTS) OF THE CONVENTION TO BE ELABORATED IN RESPONSE TO THE INVITATION OF THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES, WITH REGARD TO THE IMPLEMENTATION OF UN GENERAL ASSEMBLY RESOLUTIONS 74/247 AND 75/282.

Nigeria believes that to effectively respond to the fast-evolving threats of cybercrime, there is an urgent need to define and sanction criminal conduct in cyberspace, improve synergy in trans-national policing capabilities, improve procedural tools and reform/enhance international cooperation, whilst respecting human rights. Thus, the elaboration of a UN convention on the subject-matter at this time must focus on the fight against cybercrime and not attempt to cover cyber security and other cyber related matters that are politically volatile and are better addressed in other UN for a. It is imperative that the negotiations of the new convention must be a transparent, inclusive, and consensus-driven process, that would engender wider acceptability/adoption of the resultant convention.

1. SCOPE:

The new cybercrime convention should create a legal and institutional framework to counter cybercrime, that includes the following elements:

i. Criminalization of substantive cybercrime offences- define and sanction cyber-dependent crimes, which are crimes in which a computer or data is the target of the criminal activity, and certain cyber-enabled crimes, as well as the laundering of proceeds of cybercrime,

ii. Provision of procedural powers for the investigation and prosecution of cyber crime offences established, as well for obtaining and sharing electronic evidence of other criminal offences,

iii. Provisions / measures for sustainable capacity building and technical assistance,

iv. Provisions/measures for the recovery of the proceeds of cybercrime, and restitution,

v. Provisions/measures for improved LEA to private sector collaboration and coordination,

vi. Provisions/measures for enhanced international cooperation in relation to the above matters, including direct cooperation with ISPs; and

vii. Provisions/measures to prevent cybercrime and increase awareness, including working with civil society organizations, the private sector, service providers, academia, and research centres.

2. OBJECTIVES:

The new convention should aim at the following objectives:

i. A common understanding of established baselines for substantive cybercrime
offences, procedural powers, and international cooperation to fight cybercrime.

ii. Promote criminalizing offences in a technology-neutral manner to ensure that the substantive criminal provisions address not only present-day technologies and criminal techniques, but future technologies and techniques also.

iii. Establish authorities and capabilities to collect, obtain and share electronic evidence of cybercrimes and other offences consistent with due process and the protection of human rights and fundamental freedoms.

iv. Promote and facilitate international cooperation in the fight against cybercrime and eliminate safe havens for cybercrime perpetrators.

v. Promote capacity building and technical assistance to strengthen the law enforcement capacity to address cybercrime, as well as the usage of existing institutional capacities such as INTERPOL databases.

vi. Promote Member States' utilization of multilateral instruments that have already proven their usefulness in the fight against cybercrime, such as the Council of Europe Convention on Cybercrime and the nexus with existing UN treaties in the field of crime prevention and criminal justice, in particular the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption.

vii. Promote practitioner-level intergovernmental and multi-stakeholder process for trusted information sharing to identify future cybercrime trends, threats, and mitigations, and

viii. Establish a mechanism to monitor/facilitate the effective use and implementation of the Convention, the exchanges of information and consideration of any reviews and/or future amendments.

3. STRUCTURE:

In addition to the preamble, clear definitions, and appropriate final provisions, it is considered important that the following elements form part of the structure of the new convention:

i. General provisions/objectives and application,

ii. Cybercrime Prevention measures, like those found under the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption, for instance provisions on awareness-raising and educational initiatives.

iii. Substantive cybercrime offences and penalties,

iv. Procedural law provisions and general investigative powers,

v. Safeguards to ensure that law enforcement activities comply with international human rights,

vi. International cooperation in combating cybercrime -both formal and informal international cooperation for the detection, investigation, and prosecution of cybercrime as well for obtaining electronic evidence of other criminal offences,

vii. Provisions for capacity building and technical assistance to enhance the skills of practitioners and strengthen capacity to address cyber crime.

viii. Provisions for practitioner-level multi-stakeholder collaboration for trusted sharing of information and experiences with relevant stakeholders.

ix. Provisions for an established mechanism to monitor/facilitate the effective use and implementation of the Convention, the exchanges of information and consideration of any reviews and/or future amendments.