Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Second Intersessional Consultation

Technical Assistance to developing countries towards Countering the Use of ICT for criminal purposes

By John Ede.

Abuja, Nigeria. June 2022

Thank you Chair for the flour,

Excellencies, thank you for having me here.

Recall that, The World Health Organization on March 11, 2020 declared the COVID-19 a global pandemic. The world challenged by an unprecedented humanitarian crisis from threat of conflict, climate change and then Covid-19. Countries and cities caught 'unprepared' implemented lock-down measures as proactive and preventive strategies to contain the spread of Covid-19; increased dependence on digital devices and internet systems, local governance stretched to its limits, development suspended, economies grounded, businesses shutdown, with Air, Land and Sea transportation restricted, foreign workers evacuated back to their countries, millions of jobs lost, and huge revenue and funding cuts in the race to manage Covid-19. There was increase in the dependence on digital technology for work, education, shopping, and business transactions, virtual and digital ways of working became the new normal.

With the growing popularity of IoT (Internet of Things), people created 1.7 MB of data every second, approximately 44 zettabytes of data was generated in 2020, we create roughly 2.5 quintillion bytes of data.. By 2022, it is projected that 70% of the globe's GDP will have undergone digitization. Every day, 306.4 billion emails are sent, and 500 million Tweets are made. There is a spike in digitalization and the use of technology globally, thanks to Covid-19, people connect, work, learn, do business and communicate more via mobile phones and computer devices. According to GSMA real-time intelligence data, there are now over 10.57 Billion mobile connections worldwide.

Regrettably, Phishing Scams, Vishing and Smishing, Technical Support Scam, Authorized Push Payment (APP) Fraud were largely perpetuated by corroboration between insiders and the outside organized criminal network, to commit crimes i.e. source countries, transition countries (safe havens), and destination countries (collection or end users). Fraud and cybercrimes witnessed a spike reaching a point of 'global security emergency' with Britain's main bank reported £754m stolen from customers in the first half of 2021, in India, more than 83,000 banking frauds amounting to Rs 1.38 trillion took place during 2020-2021. Newly released Federal Trade Commission data shows that consumers reported losing more than $5.8 billion to fraud in 2021, an increase of more than 70 percent over the previous year. The FTC received fraud reports from more than 2.8 million consumers last year, with the most commonly reported category once again being imposter scams, followed by online shopping scams. According to the Association of Certified Fraud Examiners, organizations globally lose 5% of their revenues to fraud. This amounts to nearly $5 trillion lost every year.

We provide the following recommendations deliver technical assistance:

- ✓ Support countries in terms of increase in terms of ICT systems training and support, especially in Artificial intelligence and cyber security, while also building the capacity of staff member of relevant security and law enforcement officials in the technicalities of innovative technology. Calling on developed countries to support and assist developing countries, if we must achieve sustainable progress.
- ✓ There is the need to design a model framework, guide, or action plan to promote inter-country and inter-regional synergies, collaboration and coordination in terms of intelligence gathering in cyber security and profiling against the use of ICT for criminal purposes. I am happy to join and participate in the working group or the team to develop this model.
- ✓ Encourage and galvanize private sector participation towards achieving progress in the fight against the use of ICT for criminal purposes by mobilizing increased investments in data management and security, intelligence gathering and sharing and supporting the efforts of security agencies since private sector are the telecomm operators, the banks and financial institutions, the technology companies, base stations and mast operators, satellite systems operators and the internet service providers.
- ✓ Identify, recruit and build the capacity of young people, ‘the tech generation’ to use ICT for good and galvanize their support to counter the use of ICT for criminal purposes.
- ✓ Anti-fraud campaign to raise awareness on the use of ICT, and how to detect criminal activities.

With these, thank you for your kind attention, and to the organizers of this 2nd round of consultation for having me, I wish you a fruitful discussion.

Thank you