CH. 2 TECHNICAL ASSISTANCE

As one of the main mandates, ITU has been carrying out various mechanisms for ‘technical assistance’ on ICT and its security *inter alia*: for instance, on-going training and capacity building courses on *Emerging Cybercrime Trends: Cybercrime Investigation & Mobile Forensics*[^1] which presents a detailed methodological approach to understanding trends in cybercrimes and how cybercrimes can be investigated, under ITU Academy platform among many others in close partnership or international cooperation with multi-stakeholders including UNODC, Interpol, World Bank, European Commission, Microsoft, KISA and Korean Prosecution Service and so on.

In fact, ITU’s existing *Resolution 96* for *combating counterfeit ICT devices*[^2] instructs ITU to assist developing countries in preparing human resources to combat the spread of counterfeit and tampered ICT devices, by providing capacity-building and training opportunities.

[^1]: Emerging Cybercrime Trends: Cybercrime Investigation & Mobile Forensics | ITU Academy

[^2]: Resolution 96 - (Hammamet, 2016) - ITU Telecommunication Standardization Sector studies for combating counterfeit telecommunication/information and communication technology devices
Thus, as for Questions 26, 28, and 31 inter alia on Technical Assistance in the guiding questions (A/AC.291/13), considering ITU’s international legal instruments such as International Telecommunication Regulation\(^3\), its Article 6 on Security and robustness of networks inter alia, and its various capacity building courses, as well as UN Personal Data Protection and Privacy Principles, we propose in the International Convention that the States Parties seek ways to

1. identify the specific needs for countries – developing countries inter alia – to ensure the security of international telecommunication networks in countering the use of ICT for criminal purposes with regular updates with a view to fast-evolving technologies,

2. develop physical and virtual educational and training programmes, and organize joint workshops and joint coordination activities to enhance user awareness of risks in cyberspace and combat cybercrimes, and

3. develop and implement individual and institutional capacity building to ensure secured cyberspace and protect vulnerable or marginalized individuals and groups including children,

taking into account the UN Principle based on non-discriminatory and gender sensitive manner, in close cooperation with multi-stakeholders including private sector and academia together especially in view of their expertise on fast evolving technologies with constant innovation.

Further considering the mandates of ITU, hereby, the relevant technical tools or mechanisms such as voluntary international standards with training and capacity building under Resolution 44 on Bridging the Standardization Gap\(^4\) are ready to share and support for the relevant guiding questions contributing to Technical Assistance inter alia in the new International Convention.

Thank you, madam chair and delegates, for the kind attention and consideration.

---

\(^3\) S-CONF-WCIT-2012-MSW-E.docx (live.com)

\(^4\) Resolution 44 - (Rev. Geneva, 2022) - Bridging the standardization gap between developing and
developed countries (itu.int)