Inter-Governmental Expert Group on Cybercrime (27-29 July 2020), Vienna

Statement from Sri Lanka

Mr. Chairman,

Sri Lanka recognizes the value of the work of the IEG, established pursuant to the UN GE resolution 65/230. We appreciate the opportunity to comment on Chapter 7 & 8 of the Draft Comprehensive Study on Cybecrime.

In 2007, the Sri Lankan Parliament enacted the Computer Crime Act and strengthened the legal system in its fight against Cybercrime. This piece of legislation while creating substantive offences, makes provisions for investigations as well as extradition, mutual legal assistance and also contains provisions for Interception, real time collection of Subscriber Information & traffic data as well as to make preservation requests with appropriate safeguards based on international standards. It is important to note that the applicability of the provisions of this law has been extended to situations where the accused commits the offence while being outside Sri Lanka or the computer or the computer system affected is situated outside Sri Lanka or the facility or service used in the commission of the offence was outside Sri Lanka or loss or damage was caused outside Sri Lanka to a person outside Sri Lanka. Further, offences under this Act are considered Extraditable Offences and for the purposes of Extradition Law such offences are deemed not to be offences of political character.

Sri Lanka is committed to the prevention of crime in all its forms and manifestations at the national level, as well as to enhance bilateral, regional and international cooperation and combat transnational organised crime, including cybercrime. We wish to emphasize the importance of international cooperation in criminal matters, including on extradition and mutual legal assistance for which practical measures are required to facilitate cooperation.

On 7th March 2014, the Cabinet of Ministers took a decision for Sri Lanka to join the Budapest Cybercrime Convention and Sri Lanka became a state party to the said convention, effective 1st September 2015.

Securing electronic evidence from Foreign service providers is vital for the investigation and prosecution of Cyber Crime offences. Since this evidence is located in many jurisdictions, the need for more effective international cooperation is paramount. Sri Lanka has been able to use the Budapest Convention for meaningful and effective international cooperation to gather electronic evidence even in terrorism related offences.

Within the Police Department a specialized "Cyber Crime Investigations Division" has been established. This functions as the 24/ 7 contact point under the Budapest Cybercrime Convention. This unit was upgraded thanks to the technical assistance provided by the Republic of Korea.

The Mutual Assistance in Criminal Matters Act No. 25 of 2002 (MACMA), which deals with International cooperation, has been incorporated by reference into the Computer Crimes Act. This Legislation was recently updated by Amending Act No. 24 of 2018, whereby key features of Article 16, Article 17 as well as Article 29, 30 and 31 of the Budapest Convention to brought into effect in Sri Lanka.
Therefore, Sri Lanka would recommend :-

(a) The need to use existing instruments such as the UN Convention on Transnational Organised Crime (UNTOC) and Budapest Convention on Cybercrime as frameworks for effective international cooperation.
(b) Countries should continuously update domestic legislation on cybercrime and electronic evidence based on existing international standards
(c) Countries should continuously benefit from networks of law enforcement practitioners, including 24/7 networks.

In relation to Prevention of Cybercrime, Sri Lanka has taken effective measures to address issues in a comprehensive manner by adopting a comprehensive Cyber Security Strategy. Several thrust areas are being implemented by Sri Lanka CERT under this strategy with guidance from ICT Agency of Sri Lanka (ICTA) and other Regulatory entities such as Telecommunications Regulatory Commission of Sri Lanka (TRCSL) and Central Bank of Sri Lanka (CBSL).

Sri Lanka CERT also coordinates at an international level with AP – CERT and FIRST and has established sectoral CSIRTS with the Banking Sector and Education Ministry to carry out effective mitigation and prevention measures. An ISP CSIRTS will also established by the TRCSL as part of this strategy.

A series of capacity building programs on Cybercrime & Electronic evidence, covering the Judiciary, the Attorney General's Dept and Police Units, have focused on enhancing Enforcement and investigation methods. These are being carried out under the GLACY Project, which is being implemented by ICTA in partnership with Sri Lanka CERT, with support from EU and Council of Europe. This capacity development program have enhanced the ability of our Law Enforcement officials to adopt more effective "standard operating procedures", based on good practices and experience as well as lessons learnt from other Countries.

Recommendations on Prevention

- Countries should develop solutions for direct cooperation with service providers while meeting safeguards, including data protection, requirements.
- Recognize the work underway on the 2nd Additional Protocol to the Budapest Convention that will facilitate cooperation with the private sector.
- **Embark on structured and more effective capacity building programs on Cybercrime & Electronic evidence, covering the Judiciary, the Attorney General's Dept and Police Units..**

Finally, we wish to request Countries to work together towards a consensus based approach to harmonization of global norms and standards governing cybercrime.