

## **Signing the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence**

- The Deputy Secretary General of the Council of Europe
- The Chair, Vice Chair and experts of the Cybercrime Convention Committee
- Executive Secretary of the Cybercrime Convention Committee
- Your Excellency's, Ladies and Gentlemen

It is an honour and a privilege to address you this morning in these magnificent surroundings at assembly hall of the Council of Europe (COE), before a distinguished group of cybercrime experts, representing all continents of the world.

I thank the Council of Europe for inviting me and for extending gracious hospitality to my delegation from Sri Lanka. We are delighted to be the first country in South Asia to sign the 2<sup>nd</sup> additional protocol to the Budapest Cybercrime Convention. As you know, we were the first country in South Asia to join the Convention in 2015.

Since becoming a state party, we have been able to improve our response and capability to combat cybercrime. Sri Lanka has benefitted greatly from a large number of capacity building programs on Cybercrime & Electronic evidence, covering the Judiciary, the Attorney General's Dept and Police Units. These were implemented under the Global Action Against Cybercrime ("GLACY") Project, funded by COE & the EU and implemented in partnership with ICT Agency & Sri Lanka CERT. These capacity development programs have enhanced the ability of our Criminal Justice officials and helped them adopt on good practices, based on experience & lessons learnt from other Countries, as witnessed during the immediate aftermath of the Easter Sunday tragedy. We thank the COE for the support extended to Sri Lanka through these capacity building initiatives.

Cybercrime is evolving rapidly and has become a global threat impacting all countries. The number of victims of cybercrime and the importance of obtaining justice for those victims are increasing day by day. Governments have the responsibility to protect society and individuals against crime (both offline and also online), through effective criminal investigations and prosecutions.

Securing electronic evidence from foreign service providers is vital for the investigation and prosecution of modern-day criminal offences, but it has become increasingly

challenging to obtain them. Since evidence is located in many jurisdictions, the need for more effective international cooperation is paramount. As such, additional measures are needed to lawfully obtain such evidence in order to enable an effective criminal justice response and to uphold the rule of law. Further, co-operation between States and the private sector is vital for the success of modern-day investigations.

The 2<sup>nd</sup> Additional Protocol to the Budapest Cybercrime Convention is the most significant international law achievement, which provides the most effective response to address these challenges. This new instrument also contains human rights and rule of safeguards, including specific provisions on Data Protection.

The lessons learned during the negotiation of the 2<sup>nd</sup> protocol, helped our Sri Lankan experts formulate and enact the first Data Protection Legislation in South Asia, through Act, No.9 of 2022. The safeguards contained in this new Act are in line with the 2<sup>nd</sup> Additional Protocol. Sri Lanka remains committed to review other domestic legislation, including the Computer Crimes (2007), to make suitable amendments to ensure compliance with this new instrument, prior to ratification.

Finally, I wish to express my country's gratitude to the Chair, Vice Chair, the Executive Secretary, and Members of the Cybercrime Convention Committee for their dedicated efforts to negotiate and formulate this landmark new instrument. This is an outstanding contribution towards humanity, which will ensure that the Budapest Convention remains effective and relevant to deal with challenges of our contemporary digital era.