**UN Intergovernmental Expert Group on Cybercrime (27 – 29 July 2020)**

**Intervention Alexander Seger, Council of Europe**

The Council of Europe welcomes that this 6th Meeting of the Expert Group on Cybercrime is being held in spite of the COVID-19 pandemic.

The massive increase in COVID-19 related cybercrime underlines the relevance of effective measures against cybercrime, and why this Expert Group is needed now more than ever as a forum for dialogue and common responses to this challenge.

Two recommendations here:

- Underline the value of the Expert Group as a forum for dialogue and sharing of experience on responses to cybercrime.

- Additional international responses should be agreed upon by consensus to ensure that they are applied in practice by the largest number of States and organisations.

In 2013, the Expert Group had reached broad agreement on the need for capacity building as one of the most effective ways ahead. That initiated the mobilization of large resources for capacity building by many organisations.

For example, it encouraged my own organization, the Council of Europe, to establish in 2013 a Cybercrime Programme Office in Romania which has only one purpose: to support capacity building on cybercrime worldwide. With funding from the European Union, the US, Japan, the UK, Estonia, the Netherlands and other donors we have since supported more than 1000 activities with more than 120 countries.

Recommendation:

- Encourage further capacity building efforts as the most effective way ahead to counter cybercrime. And in this connection, recognise the impact that the Expert Group has already had and should also have in the future in this respect.

The vast majority of States worldwide have undertaken reforms of domestic legislation on cybercrime, often in line with the Budapest Convention.

Three recommendations here:

- States are encouraged to continue their reforms of domestic legislation in line with international standards, including the Budapest Convention.

- Criminal justice measures against cybercrime need to meet rule of law and human rights requirements. States need to ensure the free flow of information and the rights of individuals to express their views and access and share information. Restrictions need to be narrowly defined to address situations of criminal misuse. Cybercrime should not be used to legitimize the fencing in of a free and open Internet.

- Any future international response will need to be consistent with reforms already undertaken by countries worldwide and with international standards that have guided such reforms, that is, the Budapest Convention.

Criminal justice practitioners everywhere underline as their top priority the need for direct cooperation with service providers to obtain subscriber information.

The Budapest Convention already provides a partial basis for such cooperation. Solutions are also needed for access to so-called WHOIS domain name registration information.

The future Prototocol to the Budapest Convention will hopefully offer a more complete solution for direct cooperation with private sector entities. We hope that this Protocol will become available in the course of next year.

Thank you.