ROMANIA - <u>Prevention</u>

Cyberspace has had a huge impact on all components of the human society. An open cyberspace has encouraged social and political relations at all levels, and has broken down barriers between countries and citizens, enabling the exchange of information and ideas on a global scale.

While the digital world brings enormous benefits, it is also vulnerable. Cyberspace incidents or crimes are growing and could disrupt providing of essential services. Threats may have different origins, including criminal, politically motivated, terrorist or state-sponsored attacks.

In this context, cybercrime prevention has become an important component of national policies based or inspired **by the international legal instruments, such as Budapest Convention**, adopted to harmonize concepts and measures to prevent and counter cyber-attacks and threats, as well as to diminish the vulnerabilities of cyber infrastructures, to obtain finally effective management of all risks.

First and foremost, **the fight against cybercrime is a global fight that aims at protecting and strengthening cyber resilience in fully respect of fundamental rights and liberties of the persons using, owning or facilitating the use of any cyber infrastructures.**

A comprehensive approach to fight against cybercrime includes beside funding of technical development of software and hardware solutions that can be implemented at a large scale to make Internet and related technologies of communication always available and safer for its users, **making better the cooperation in all sectors and at all levels between the actors involved at national and international level.**

In sum, aware of the importance of the issue of cybercrime and efforts already posed in combating cybercrime, **Romania has the following recommendations:**

- **First recommendation is to continue developing solutions for direct cooperation with service providers while meeting rule of law and human rights requirements, including data protection.**

The Budapest Convention already facilitates cooperation with service providers on the basis of Article 18. In addition, the current work on the 2nd Additional Protocol to the Budapest Convention will further facilitate cooperation with the private sector.

- **The second recommendation is to continue** increasing the efforts to sustain capacity buildings programmes as the most effective way ahead to counter the problem of cybercrime.

- **Finally, the third recommendation is to acknowledge** that commitment of governments to implement international agreements - such as the Budapest Convention and UNTOC - creates a solid basis for donors to provide support to capacity building projects. **Thus, <u>it is crucial that future instruments should avoid conflicts with exiting standards.</u>**

An outstanding example is the assistance provide by the EU, the Council of Europe and other donors and organizations to States that decided to join the Budapest Convention.