Madam Chair,

Preventive measures are a vital complement to existing cybersecurity systems, with the aim of eliminating — at the source — the criminal use of information and communication technologies (ICTs). The Holy See thus favors the inclusion of strong provisions to assist States both in building a culture of information security and in protecting critical infrastructure from attack. At the same time, it must be stressed that any State intervention aimed at creating a safe cyber environment should scrupulously respect basic human rights that recognize that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.”

Madam Chair,

Our Delegation would like to share some remarks on three areas that, we believe, should be given particular consideration in this section.

First, education about ICTs should be made a priority, enabling users to make a critical appraisal of both the potential benefits and risks inherent in these technologies. Educational curricula should include modules on the development of ICT-related skills and cyber hygiene best practices, as well as on the broader issues of online safety, data privacy and anonymity. In this regard, children require particular attention, as they are at greater risk of victimization, especially through the production and distribution of sexual abuse materials, including child pornography. Indeed, a greater understanding of

1 UDHR, Art. 12
this issue “is urgently required [... as] one feature of today’s technological development is that it is always one step ahead of us.”

Second, it is important to involve, as appropriate, relevant stakeholders, such as the private sector, academia and other members of civil society with proven expertise to contribute to preventive measures, especially with regard to public engagement. Their knowhow can prove helpful in identifying problems, developing policies and guidelines, and crafting effective, culturally appropriate information campaigns and programs to be considered by States, in accordance with their national priorities.

Third, States Parties should develop and maintain a high level of protection and resilience with regard to critical infrastructure, such as hospitals, schools, energy systems and water supplies. To that end, international cooperation and technical assistance from those States with greater experience and knowhow may well prove invaluable. In addition, the criminal use of ICTs to attack key infrastructure may easily have a devastating impact on innocent populations, risking lives and causing irreparable damage. States Parties should, therefore, adopt national and supra-national policies to ensure the effective protection of critical infrastructure.

Madam Chair,

The convention should also consider the particular needs of victims of crimes committed through ICTs. States Parties must uphold the victims’ rights, assist them in accordance with their specific needs and protect them from further harm. These tasks take on special urgency with regard to child victims. Assistance programs should enable victims to engage with law enforcement and judicial authorities, to participate in criminal proceedings without fear of retaliation, to seek restitution and to receive other forms of needed support. For these reasons, the convention should include robust victim assistance provisions, as laid out in article 25 of the UN Convention against Transnational Organized Crime.

I thank you, Madam Chair.

______________________________

2 Pope Francis, Address to the participants in the congress on “Child Dignity in the Digital World”, 14 November 2019