Statement of the Republic of Slovenia

at the second session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Item 4: Provisions on criminalization (1st group of guiding questions)

Wednesday, 1st June 2022

Madam Chair,

We would like to thank you for the guiding questions that allow the delegations to express the positions on specific topics in a structured manner. Slovenia fully aligns itself with the statement delivered yesterday on behalf of the European Union and its Member States and would like to make the following remarks in its national capacity.

Slovenia believes that only the offences that serve a legitimate goal, that are necessary and proportionate should be included in the Convention. Such an approach will ensure a required common understanding of cybercrime and application of provisions on criminalization regardless of the type of a computer system targeted by offenders or their motivation to do so. Such an approach would also allow full protection of human rights, a standard that may be diluted if the provisions on criminalization were to become too broad and ambiguous.

Slovenia also believes the Convention should not include crimes that are already included in existing international conventions, nor content-related crimes. The latter are extremely delicate as they could seriously interfere with human rights of persons as well as constitutional systems of State Parties as it was yesterday explained by the representative of the Office of High Commissioner for Human Rights

Madam Chair,

to respond to your questions: regarding elements of the offences, we consider that the substantive provisions of the Convention should only apply when an offender is acting with intent and without right to do so. In this regard, the Convention should provide a minimal common standard, allowing a degree of flexibility for the State Parties when implementing its provisions, including a possibility to incorporate additional elements of an offence, such as dishonest intent or an act resulting in serious harm or threat as well as to foresee relevant aggravating or mitigating circumstances.

Such an approach is also relevant for cases in which a suspect would technically commit an offence, but would not do so in order to cause harm – for example, when conducting a research or to detect weaknesses in a computer system, without prior authorization. To protect the researchers and ethical hackers, the State Parties should be able to lay down rules on the relevance of such circumstances in line with their national systems, allowing law enforcement and judicial authorities to make a proper assessment and decision on a case-by-case basis.

Furthermore, to ensure proportionality of criminalization, intentional infringement of a security measure, such as an abuse of a password or of the known deficiencies in a computer system security, could be included as an element of an offence of illegal access. For the rest of the cyber-depended offences, we consider that the inclusion of infringement of security measures is not relevant.

In relation to questions four and five: we believe that the conducts which are solely derivatives of the core cyber-dependent crimes should not be included in the Convention as separate offences. However, certain distinct elements of such conducts could be regarded as aggravating or mitigating circumstances that the States Parties may take into consideration when drafting their implementing legislation; this

could, for example, be the case when access or interference relates to a critical information infrastructure.

With regard to the use of terms, we believe that the appropriate terms to use would be “without right” and “illegal” or “unlawful”; the latter two being synonymous. Furthermore, as regards the term data versus digital information: In computing, **data** is any sequence of one or more symbols and includes text, computer programmes, pictures, video, sound. Data requires interpretation to become information. So, in our view the term “data”/”computer data”, when referring to what has been processed by any ICT device, is more appropriate to be used than the term digital information.

Madam Chair, in conclusion, allow me to briefly add the voice of Slovenia to all those delegations who, throughout the process, aspire and seek to find a consensus-based solutions of the committee.

Thank you, Madam Chair.