

Thank you Madam Chair,

The State of Israel wishes to thank the Chair and the secretariat for the highly useful guiding questions presented in the 1st cluster of criminalization provisions. With respect to some of the question, we prefer to submit our opinion in writing at a later date,[after hearing the responses and explanations of other member states with respect to the texts suggested by them].and we will present here some of our positons on these issues:

On the first question Israel believes that acts criminalized under the Convention should be those of intent, while maintaining some flexibility for States to make more specific requirements in accordance with their internal laws. As for the issue of providing protection for cybersecurity researchers and other professionals working in cyber security field, Israel would like to echo the position made by Australia and several other MS in this regard and we are open to working together in order to find agreed language that will lend these professionals the appropriate protections under the convention.

Turning to the second question Israel is in agreement with many other member states that have mentioned that the conduct in itself should be criminalized, regardless of the harm that it may or may have not caused. As noted by other states, the question of harm may be regarded as an aggravated circumstance and be relevant for the issue of sentencing.

As for the question regarding the infringement of security measures and whether it should it be considered as a condition for establishing some conducts as an offence, Israel is of the view that the infringement of security measures should not be considered as a condition for criminalizing certain conducts.

Considering the proposed provisions on “Obstruction of a computer, program or data”, “Attack on a site design” and “disruption of information and communications technologies networks”, as forms of illegal interference, Israel agrees with the UK and other member states that

offence of illegal interference should be drafted in a broad manner, and each state will maintain the flexibility within its national legislation to define this issue.

On the question of how the convention should deal with the “unauthorized access to or interference with a critical information infrastructure”, similar to the United States, the UK, Australia and other member states Israel holds that such conduct falls within other offences. We further believe that the purpose of this convention is to deal with cyber-crime only, and that it is not meant to, and should not, deal with any matters pertaining to national security.

As for the difference between “data” or “digital information” as the appropriate term to be used, Israel does not favor the use of the concept of "digital information" as we fear it might be overly broad and may also refer to the content. In the Israeli Penal law, there is a clear distinction between the two. Therefore we suggest using the term Computer Data as it also has been used and tried successfully in other instruments and we do not believe there is a substantive reason to depart from it.

Thank you Chair.