Misión Permanente de Costa Rica ante las Naciones Unidas
211 E. 43rd Street, Room 1002, New York, NY 10017. Tel: (212) 986-6373

III Session of the Open Ended Working Group on security of and in the use of information and communications technologies 2021-25.

Nueva York, Julio 12 2022

Delivered by Minister Counselor José David Murillo.

Dear Mr President,

I requested the floor to express our gratitude to you and your team for conducting this OEWG. The first two sessions of this substantive group took place in a challenging geopolitical environment that has only increased the threats to trust, peace and security, but your leadership and countless consultations have been able to move us forward.

Costa Rica also wants to recognize your hard work in presenting before us this document. As a general comment we believe it does capture the essence of the debates throughout the first two sessions, also, reflects the different proposals and preferences of the States that have taken the floor or have submitted their written contributions.

As mandated on the 75/240 resolution, the OEWG must submit annual progress reports to the General Assembly for adoption by consensus; We stand ready to start negotiations on this text in a constructive fashion.

First and foremost, Costa Rica wants to recognize three core elements in the text: *the importance given to the* ***participation of interested stakeholders***; ***the inclusion of approaches from a regional and sub regional level***, and the ***continuation given to proposals and debates from the previous negotiations***, with special attention to the resolution **76/19**, (that includes the 2021 report of the Open-ended Working Group and the 2021 report of the Group of Governmental Experts); as well as the Chair's Summary in the 2021 OEWG.

Costa Rica also considers it is a positive sign that the document intends to include the **implementation part** into the discussions, and therefore would like to refer to the topics that would be a priority for my delegation:

Existing and Potential Threats: The discussions on protection of Critical Infrastructure and Critical Information Infrastructure. While those discussions are undoubtfully a governmental process, we do see the need in having representatives from regions and sub regions as well as interested stakeholders in those discussions. We would also prefer to see the discussions of ransomware reflected on this part of the document.

Rules, Norms and Principle of Responsible State Behaviour: We want to emphasize the importance of the voluntary national survey of implementation and the report of the SG on development in the field of ICTs on the context of international security, this in order to address the discussions on these topics and contribute to better understandings among member states.

International Law: We want to emphasize the importance of the voluntary national survey of implementation and the report of the SG on development in the field of ICTs on the context of international security, this in order to address the discussions on these topics and contribute to better understandings among member states. Also, in Costa Rica's opinion, the paragraph 5a has a value to address the content of international law. We would also support the inclusion to Humanitarian International Law on this part of the text.

Confidence Building Measures: The Directory of Global Points of Contact as well as an intersessional meeting with States and interested stakeholders to explore the development and implementation of CMBs will be an important asset to the mandate of the OEWG. The Use of the UNIDIR Cyber Policy Portal will also contribute to strengthen the role of the UN in the process and hence multilateralism.

Capacity Building: The importance of developing cooperation programs within States, States and the UN, States and regional and sub regional organizations, States and interested stakeholders. Those cooperation programs shall include both, the content and the funding of the programs. A great example of this is the Cybersecurity Capacity Maturity Model.

I thank you.