Statement delivered in Spanish on March 7, 2024

7th Substantive Session - OEWG on security of and in the use of ICTs

JOINT STATEMENT ON BEHALF OF A GROUP OF LATIN AMERICAN STATES ON "CAPACITY BUILDING"

(English translation)

Chair:

I take the floor on behalf of the following Latin American region delegations: Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Paraguay, Peru, Uruguay, and my own delegation, Argentina.

We would like to take this opportunity during this seventh session to reiterate our shared position on capacity building, as well as to highlight the topics we consider a priority and, therefore, require concrete actions.

Likewise, with a view to preparing the third Annual Progress Report of 2024, which will be circulated for this Working Group's consideration in July, **we will present proposals for language aimed at its inclusion in the next Annual Progress Report.** *(see pag. 6 and 7 bellow)*

Chair,

Addressing capacity building from a comprehensive, holistic approach, and based on Human Rights is essential to ensure that this Working Group can present proposals that translate into lasting and effective achievements, for the benefit of all. For this reason, our delegations welcomed, last December, the recognition by the 2023 Annual Progress Report that capacity building inherently constitutes a confidence building measure.

Recognizing the digital divide and, therefore, the crucial role of capacity building in a broad sense, is fundamental. The digital transformation needed to overcome this

divide is part of the path towards our shared goal: a resilient, open, safe, stable, accessible, peaceful, free, and interoperable cyberspace for all.

Leading our group's efforts towards the development, strengthening, and constant updating of each member's skills, considering our diverse starting points, is essential to identify and mitigate cyber risks.

Adopting an inclusive and equitable approach would help to improve digital security not only at an individual level but also collectively.

In this context, we consider that the future permanent mechanism for institutional dialogue should incorporate clear and precise guidelines on ongoing capacity building, to ensure it is truly open, inclusive, transparent, sustainable, and flexible, capable of evolving based on the differentiated needs of States and the assessment of the ICT environment.

The approach we propose, towards an action-oriented capacity building, especially regarding the implementation of norms for responsible state behavior in cyberspace, is based on the premise that ***no State will be secure until we all are secure***.

Furthermore, aiming for the safe, effective, and meaningful participation of all States in cyberspace, we believe that the implementation of the responsible behavior framework should be complemented with the promotion of innovation, technical assistance for capacity development, and technology transfer in accordance with existing international law and considering the needs of developing countries. This would contribute not only to the well-being and economic and social development of our countries but also to the application and adoption, on an equal footing, of the cumulative and evolutionary framework of responsible behavior in the use of ICTs.

We highlight the role of multilateral organizations and regional and sub-regional initiatives as key coordination and cooperation platforms among States, as we understand that their experience in designing specific training programs provides significant added value to the capacity building process.

Likewise, we encourage States to continue supporting capacity building initiatives, in accordance with the principles of Annex C of the 2023 Annual Progress Report, and to foster collaboration with regional, sub-regional organizations, and other stakeholders, such as the private sector, NGOs, academia, and civil society. These collaborations can strengthen regional and international cooperation, as well as North-South, South-South, and triangular cooperation initiatives in science, technology, and innovation, promoting specific technical assistance actions for capacity building that especially consider the needs of developing countries.

In summary, Chair, we consider cooperation and capacity building to be fundamental pillars for building a secure and resilient cyberspace. It is imperative that we continue working together, sharing knowledge, experiences, and resources, to foster an inclusive and equitable digital environment for all. International cooperation in capacity building is not only essential to close the digital divide but is also crucial for maintaining international peace and security.

In light of the above, Chair, and with a view to drafting the **2024 Annual Progress Report**, our delegations would like to make the following "recommended measures" proposals to be incorporated into the report on the progress made in the working group's discussions on agenda item 5, specifically in the section titled "capacity building":

1) ***Encourage States that are in a position to do so, to promote technical assistance including discussion workshops, training and capacity-building courses on:***

- ***cyber diplomacy and responsible state behavior in cyberspace, including the application of norms, confidence-building measures, and the application of international law.***
- ***critical infrastructures, which include methodologies for States to identify essential sectors and service operators as well as actions aimed at improving cyber incident management, from early warning, identification, remediation, and resilience building.***
- ***Application of international law in cyberspace, taking into account the fundamental importance of incorporating different perspectives into the debate and presenting doctrinal divergences regarding the modalities of its effective implementation.***
- ***Development of operational capacities in establishing and enhancing the maturity of National and sectoral Cyber Incident Response Teams (CERT/CSIRTs).***
- ***Existing and emerging threats, such as ransomware, and the cybersecurity challenges posed by new technologies, such as the uses and applications of artificial intelligence and quantum computing, among others.***
- ***Exchange of knowledge and experiences acquired, tailored to the circumstances of each country.***

2) ***Encourage States to exchange experiences on incident response protocols and the implementation of risk management frameworks that identify, assess, and mitigate potential security threats in ICTs.***

3) ***Encourage States, with the capacity to do so, to promote innovation, technical assistance for capacity building, and technology transfer in accordance with current international law aimed at strengthening cyberspace resilience.***

Finally, we reiterate that capacity building is a fundamental and cross-cutting aspect of all the topics of the GTCA. Therefore, it is important that it has a sustainable and permanent character. We believe that creating a tool that serves this purpose would be a key cooperative measure that should be considered as part of the future regular institutional dialogue mechanism.

Thank you.