Check against delivery.

Statement of Romania

within the fourth substantive session of the Open-Ended Working Group on security of and in the use of information and telecommunications technologies 2021-2025 (OEWG), established pursuant to General Assembly resolution 75/240 adopted on 31 December 2020

(6-10 March 2023)

Agenda item 5: discussions on substantive issues contained in paragraph 1 of the General Assembly resolution 75/240: ***Confidence-building measures***

Mr. Chair,

On CBMs, as well as on the rest of the agenda items, we are fully aligned with the EU statement.

Responsible state action in cyberspace is about respecting international law and taking all reasonable steps in order to mitigate risks to international peace and security. These steps include respecting voluntary norms and also engaging in confidence building measures.

We support and encourage dialogue and cooperation between members of the United Nations at a bilateral, regional and multilateral levels; we encourage voluntary exchanges of information between member states; cooperation in the establishment and between CERT-type entities responsible with mitigating the impact of malicious cyber operations; measures of legislative and decision-making transparency; the explicit declaration of doctrines; cooperation with multistakeholders; and the voluntary exchange of information and good practices of relevance for the implementation of the 11 norms of responsible state conduct in cyberspace.

In identifying the manner in which to best make use of confidence-building measures in supporting international peace and security, an ever larger set of examples and good practices have been developed at various levels, including regionally, some of which we have heard described today, coming from within the Organization for Security and Cooperation in Europe, the Organization of American States, the Association of South East Asian Nations, and the Regional Forum and the Economic Community of West African States. Their contribution to the pool of good practice in this regard is significant.

We fully adhere to the calls to actively ensure the integration of the gender component to initiatives aimed at increasing our common security, resilience, and transparency, as well as in the processes of reporting.

We are also engaged in the development and implementation of the OSCE CBMs, and fully share the view that they both show and promote resilience in times of crisis. We also highlight the example significance of the coordinated vulnerability disclosure experience.

We assess positively the clear added value of the Cyber Policy Portal of UNIDIR.

On the PoC directory, as stated before, we welcome the circulation of your document. We consider it a good base for discussions directed towards precisely identifying and agreeing on the specifics of what is needed for operationalizing such the initiative. We look forward to the dedicated discussion on the topic.

Thank you!