ICT4Peace – Input for informal OEWG on ICT Security consultation. July 3, 2024

The OEWG Chair has asked that discussion focus on the contribution that stakeholders can make to the realization of proposals by States as referenced in the Zero Draft of the 3rd APR.

ICT4Peace would stress that civil society and the private sector are already via their ongoing activity contributing significantly to the implementation of the agreed normative framework (as per para 3) and the fulfilment of many of the State proposals recorded in the 3rd APR.

Given that the 3rd APR acknowledges that "it was fundamental for all States to observe and actively implement the framework for responsible state behaviour in the use of ICTs" (para 5), the work of ICT4Peace can be seen as a means of encouraging states to achieve this implementation. Specifically, the introduction of accountability mechanisms such as our proposal for a peer-review mechanism can help incentivize states to put normative commitments into practice.

The 3rd APR "underlines the importance of the protection of Critical Infrastructure." It also flags the "escalatory" risk of offensive cyber operations that damage this infrastructure (para 29 e). ICT4Peace has long drawn attention to this vulnerability and continues to urge all states with such offensive capabilities to make specific public pledges to refrain from such attacks against Critical Infrastructure and to withdraw any malware already planted in the Critical Infrastructure of other states.

With respect to the capacity building facet of the 3rd APR, ICT4Peace has been engaged for years in cyber security capacity building, especially in its diplomatic dimension in furtherance of the capacity-building objectives referenced in the 3rd APR (para 50). Its continued educational programs can support the development of capacity on the part of states enabling them to be more effective players in the elaboration of international cyber security policy (50 h).

Part of ensuring a useful contribution by stakeholders is to approach cooperation mechanisms in an inclusive rather than restrictive manner. Why for instance promote a Global Cyber Security Cooperation Portal that is "State driven" and a "tool for States" (50 c) rather than engage fully with the existing UNIDIR Cyber Security Portal with its more open orientation to stakeholders?

Furthermore, on the subject of stakeholder participation modalities in the future Regular Institutional Dialogue, rather than trying to agree these at the upcoming July OEWG, we are in favor of these being adopted at the General Assembly in a fashion similar to that of the Ad Hoc Committee on Cybercrime Committee.

If there is to be a genuine and mutually beneficial collaboration between states and stakeholders in promoting ICT security every effort should be made to facilitate joint action and refrain from erecting new barriers to collaboration.