CyberPeace Institute

Comments by the CyberPeace Institute on the "Zero Draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security

February 2021

The CyberPeace Institute has reviewed with great interest the "Zero Draft" report of the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. We commend the efforts of all who participated in the OEWG's process, and for the Chair, His Excellency Ambassador Lauber, and his team for the high quality of this draft and the work it has taken to include stakeholder comments.

The CyberPeace Institute would like to submit the following comments for consideration. As the report is in a near-final stage, our comments reflect general concerns and points of interest throughout the "Zero Draft," rather than identifying individual points of contention section by section.

Consistent with our previous comments on the "initial pre-draft report," we would again like to emphasize the **need for a stronger human-centric approach throughout the report** and its associated dialogues and consultations. This is a priority that has been raised by UN Member States throughout the discussions, as well as by other stakeholders during the intersessional proceedings. It was to our disappointment that the focus on a human-centric approach was only mentioned in Paragraph (4) of the "Zero Draft," especially considering the challenging times we are experiencing which require a uniquely humane and holistic approach. At the CyberPeace Institute, we believe that a human-centric approach to ICT-related and cyber questions will facilitate a more comprehensive understanding of the impact of such issues on human beings, and the most appropriate response in order to create a more secure and accessible cyberspace. Without this guidance, it is easy to become lost in the technical, and even economic facets of these issues, leaving the human impact unresolved. It is for these reasons that we call for a greater recognition of the human impact of ICT issues, and the direct connection they have to the protection and promotion of international peace and security.

It was, therefore, with great pleasure that we read in Paragraph (55) of the explicit agreement on the protection of medical services and healthcare facilities under the norms related to critical infrastructure. Over the past few months, we have seen the consequences of attacks against healthcare facilities in terms of the violation of privacy of personal information, all the way through to impacted treatment, surgical, and vaccine schedules. The increasing sophistication of attacks against the healthcare sector is concerning, and so we welcome this agreement by States, which is a step closer to the protection of these essential services.

We reviewed Section C - International Law with great interest, as the advancement of international law and norms is a key pillar of our work at the CyberPeace Institute, in order to enhance human security, dignity and equity. However, we see a clear gap in actionable steps towards the advancement of international law, which influences accountability in cyberspace. As several experts have pointed out, there are clear rules in international law. However, the application of the relevant rules and the corresponding public endorsement of them remains an issue. This in turn has an impact upon the enforcement of these laws and the very practical issue of accountability. **Without a clear delineation of action beginning with the identification of relevant laws and rules, there can be no accountability in cyberspace.** This is, in our estimation, a missed opportunity by the UN OEWG. Discussions such as these need to be happening at the international level to strengthen the viability of enforcement and accountability. Until then, human security, dignity, and equity will continue to be impacted by attacks such as those perpetrated against the healthcare sector.

Further to these ideas, we believe that **the report needs to have a greater emphasis on accountability.** As difficult as a clear, public, evidence-led accountability process may be, we believe that this is essential to ensure the security of cyberspace. The issue of accountability is highlighted several times throughout the "Zero Draft," particularly in Paragraph (9) where all actors are called to uphold their duty to act responsibly in cyberspace and in Paragraph (36) where States are called to share best practices in order to support the goal of accountability and transparency in cyberspace. In addition, in several instances (namely in Paragraphs 35, 41, 58, 72, 92) States have been urged to report their views and assessments to the Secretary-General, sometimes for them to be used in the Secretary-General's annual report. While this is an important first step, we at the Institute urge those who report on their work to follow more precise requirements regarding documentation, measurement, and evidence in order for these conversations and reports to contribute to and build towards greater accountability. We also call for this information to be released beyond the walls of the UN in order for other stakeholders, such as neutral bodies, to be able to use this information to inform their work and to be more effective in their accountability efforts.

A key part of accountability in cyberspace is the question of inclusion: the inclusion of all States during international discussions; the inclusion of civil society, academia, and industry in relevant processes; and the inclusion of practitioners so they can better understand how to protect themselves from cyberattacks. Accountability is the responsibility of every stakeholder at every level of activity in cyberspace, and so the inclusion of these stakeholders in relevant discussions is the logical next step. We commend the efforts that have been taken to make the UN OEWG process, including the drafting of the report, more inclusive. This is an admirable step in the right direction and is rightly highlighted throughout the "Zero Draft" report. However, we ask that more is done by those in positions of power and privilege to include those who are not. We applaud the Programme of Action presented by several governments as a step in this direction, as they particularly aim to facilitate regular multi-stakeholder consultations in order to complement the ongoing work at the UN level.

Overall, we were encouraged to read the "Zero Draft" report put forth by the OEWG, and we were pleased to see that some of the input from other stakeholders outside of the UN process had been incorporated into this latest version. At the CyberPeace Institute, we ask that there be a greater push towards accountability, which requires an inclusive process, evidence-led reporting of attacks, and the advancement of international law. Steps have been taken in this direction, though we re-emphasize the need to keep a human focus on all these issues. We cannot afford to lose this perspective if we are to ensure and protect a secure cyberspace for all.