Submission to the first substantive session of the UN Open-ended Working Group on security of and in the use of information and communications technologies (2021-2025)

December 2021

On the occasion of the first substantive session of the second Open-ended Working Group (OEWG II) on security of and in the use of information and communications technologies (2021-2025), the CyberPeace Institute welcomes the start of the process and the opportunity to strengthen the current normative and operational framework to achieve cyberpeace. As an independent NGO based in Geneva, working to ensure the rights of people to security, dignity and equity in cyberspace, we have contributed to OEWG I and followed with great interest the OEWG II discussions so far. We believe that the decisions taken in this process must serve their ultimate objective - to maintain international peace and security - as a means to an end. The end goal is to protect individuals and enable the enjoyment of their fundamental rights and freedoms and economic and social advancement. From this perspective, we provide below three key points for consideration at the start of the OEWG II process.

To study the impact of potential threats in cyberspace should, first and foremost, mean studying and understanding how their disruptive nature impacts victims and individuals.
It's only by understanding the perspective of victims and individuals- what we, at the Institute call the human centric approach and which we documented and analyzed - we can ensure that all the areas of the upcoming work of the OEWG II, whether it be capacity building, implementation of norms of responsible behavior, or confidence building measures, will fulfill their ultimate aim.

I. Opening the discussions up to multistakeholder engagement

In the spirit of constructive contribution, the Institute shared a Statement on the value of multistakeholder engagement in the OEWG process signed by 27 organizations on 13 December 2021 and signed the Multistakeholder letter on modalities sent to the Chair on 7 December. We hope that such input is beneficial to the deliberations on modalities of multistakeholder engagement. Our statement calls for meaningful engagement of non-state actors in the OEWG process and ***reflects the specific contributions*** that the multistakeholder community can make on the topics of the agenda set forth by the Chair. These reflect the

diverse experiences and expertise that non-state actors bring to the process, from technical knowledge and field knowledge to support in building sustainable and resilient communities.

We appreciate the Chair's attention to the concerns raised regarding the modalities of engagement and urge him to work with member states towards a more substantive approach. Meaningful and substantive participation to the OEWG does not mean a meeting on the sidelines, or sporadic intersessional meetings. The inclusion of non-state actors in the discussions with member states is imperative at the time when these discussions happen, to provide timely and relevant perspectives. If we are only left to reflect on what's already been agreed, then our expertise and knowledge are not being used to their full potential, to the benefit of the process.

We urge all member states, especially those where civil society organizations struggle to partake in these important discussions, to involve and empower civil society actors in UN processes.

The issues raised during the agreements following the OEWG's deliberations have a direct impact on victims of cyberattacks, and society more generally, and we need to ensure that this perspective remains at the core of all discussions. But this is only possible if the process includes organizations that understand these human equities, study the impact of insecurity on individuals, work with victims of cyber attacks, and work to ensure that human rights and individual freedoms are respected when governments make difficult decisions about our collective future.

II. Prioritizing a human-centric approach in the deliberations

As mentioned in our review of OEWG I's Final Report, our hope was that a human-centric approach would form the basis of discussions to keep the focus on the impact of digital issues on people's lives. We believe that it is only by understanding the perspective of victims and individuals - what we at the Institute call the human centric approach - that we can ensure all the areas of upcoming work for OEWG II will fulfill their ultimate aim. The study of threats in cyberspace need to include the impact on people and society; capacity building initiatives need to be increased at the local, national, and regional levels and should include a variety of stakeholders, including civilians. OEWG II should also include concrete negotiations around actions to implement norms of responsible behavior and confidence building measures. All of these areas relate to the protection of individuals and their ability to enjoy their fundamental rights and freedoms. Just as the political and economic aspects are vital to cyber discussions, so too is the societal and human perspective.

Additionally, the protection and empowerment of civilians is directly related to OEWG II's discussions, and therefore form the core of a human centric approach. Several states have already mentioned the need to move away from theoretical discussions and to focus on practical next steps. In this way, OEWG II's ambition for an 'action-oriented agenda' can be realised. Several states have already mentioned points to this effect, including what a human centric perspective means to them. This includes an end user's confidence in products, the implementation of security by design, and the acknowledgement that technology should not violate human rights.

One way to move this human centric perspective forward in an actionable way, would be to focus on the healthcare sector as a key initiative for all the areas of work of the OEWG (capacity building, implementation of norms, studying the threat). Access to healthcare is a human right and it is the responsibility of governments to protect this critical sector. By focusing on better protecting the healthcare sector against cyber attacks, discussions around the clarification of rules and the implementation of capacity building programmes would respond to pragmatic needs on the ground and make the deliberations more tangible.

The CyberPeace Institute documented the sharp increase in attacks against the sector and analyzed the disruption they cause to individuals. The need for collective action to stop the targeting of healthcare facilities is more urgent than ever. We have seen that cyber criminals do not abide by the rules, and in fact go back on their own word to not target hospitals and medical facilities. The OEWG is a space for states to enact plans to counter such threats and to protect this critical sector.

III. Taking the work of the OEWG I forward

In our review of OEWG I's Final Report, we mentioned our hope that the next process would "...bring these discussions closer to those impacted by cyberattacks and offer new remedies to those left vulnerable." It has been flagged at several points of UN discussions that there is a clear lack of accountability in cyberspace. We at the Institute are also adamant that the lack of actionable steps towards greater accountability in cyberspace is a serious concern. Without clear guidance on how to seek accountability in the aftermath of attacks, people will continue to fall victim to cyberattacks and be unsure of their rights, as States are unclear on what actions they can take to hold malicious actors to account. This point is especially pertinent for the proposed Programme of Action, whose aim is to implement the recommendations outlined in OEWG I's Final Report.

States have mentioned that they cannot implement what has been agreed upon alone; the multistakeholder community is prepared to assist in the analysis of emerging threats, collaborate on an accountability framework, and contribute to inclusive solutions for those who face digital disparities.

The CyberPeace Institute welcomes collaboration with other non-state actors, and stands ready to organize future coordinated input. This is not a process that any one actor can pursue in a silo. By ensuring the substantive participation of non-state actors in OEWG II's process, we are sure that positive, actionable steps will be taken and the discussions will remain action-oriented.

The CyberPeace Institute remains available for additional input and support throughout the OEWG II process.