Distinguished Chair, colleagues,

The Association for Progressive Communications welcomes this opportunity to address the Open-ended Working Group and to participate in this informal dialogue with stakeholders. APC is a global NGO and network of members working in 72 countries to advance an open, secure, stable, and rights-based internet.

In our statement, delivered on behalf of ten non-governmental organisations, we take the opportunity to address each of the items in the organization of work.

People are first and foremost directly impacted by cyberthreats and operations. Therefore, as noted in the report of the Chair of the informal intersessional consultative meeting of the OEWG, it is important that both threats in cyberspace, as well as measures to address these threats are approached, understood and defined in a human-centric manner. When cyber attacks or threats are not considered from a human-centric and rights-based approach, this can lead to criminalisation of technical expertise and the prosecution of journalists and security researchers. It is also critical to consider the differential threats people face both in their use of ICTs and in the context of international conflicts because of their sex, gender identity and/or sexual orientation. Therefore, gender sensitive approaches to cybersecurity are necessary.

With regard to norms, there have been repeated calls, including at the September session of this working group, for greater adherence to the 2015 norms as well as for greater efforts to increase awareness of the norms among states. We therefore urge the development of a multistakeholder mechanism to review implementation of agreed norms, in line with the proposal made by Mexico at the September session of the OEWG. We understand that such efforts are under way in the G7 and ASEAN but believe that an inclusive approach in which all countries participate would be preferable. Because all stakeholders play a valuable role in the implementation of norms, it is essential that all are able to contribute to an implementation review mechanism, including through shadow reporting. Existing international mechanisms, in particular the Universal Periodic Review of the Human Rights Council, provide useful examples of how monitoring and implementation can be facilitated by the UN system.

We urge States to lead by example in adhering to agreed the norms themselves and provide support to others to do so. States should draw attention to acts contrary to the norms in order to increase accountability, transparency and help build habits of responsible behaviour. The development of any new norms should be done in a manner inclusive of all stakeholders and make reference to existing multistakeholder efforts, such as the work of the Global Commission on the Stability of Cyberspace.

With regard to capacity building, open, inclusive and transparent processes which engage civil society and academia are essential as they include wider perspectives and allow for more sustainable outcomes. Cyber security capacity building efforts reflect the priorities of those who design, deliver, and engage in them and it is therefore important that they institutionalise a
multistakeholder and multidisciplinary approach to tackling challenges raised by ICTs, informed by a full understanding of their social, economic impact and implications for human rights. Capacity building efforts that emerge from the OEWG should build on existing efforts, to avoid duplication and allow synergies. Principles of openness, inclusivity and transparency should also apply to confidence building measures.

With regard to international law, it is essential to reinforce that both international human rights law and international humanitarian law apply to cyberspace. International human rights law extends beyond the duties of states to include the responsibility of businesses to respect human rights and abide by their due diligence to ensure that their products and services aren’t used to violate human rights. In line with the UN Guiding Principles on Business and Human Rights, States should be willing to share information about human rights abuses by private actors and should hold private actors who enable or facilitate these acts to account.

The resolution which established the OEWG, specifically stresses that "effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations". We regret therefore that once again many representatives of organisations that do not have ECOSOC status were unable to gain accreditation for this session, replicating the situation in September. As was noted in the successful informal intersessional in December, non-governmental stakeholders play valuable roles in the documentation and verification of cyberattacks, capacity building, research, monitoring and implementation of norms, development of technical and policy standards, among many other roles. The successful intersessional also highlighted the ability of the Secretariat and Chair to identify those actors whose contributions should be sought, but who are not part of the ECOSOC process.

Any discussion with regard to future regular institutional dialogue should prioritise ensuring effective participation and consider the scope of the dialogue, inclusiveness of all relevant non-governmental stakeholders and complementarity with existing mechanisms and processes. These elements are key to the success of these discussions and their contribution to a secure and peaceful cyberspace for all.

Therefore, Chair, in summary, we urge a rights-based and inclusive approach to understanding threats in cyberspace, and acknowledgement of the importance of all relevant stakeholders to both implementation and development of measures to address cyberthreats. These principles should also apply to the development of a peer review mechanism to promote learning and review of the already adopted norms and to any future dialogue. Thank you Chair.

Access Now
Association for Progressive Communications
Derechos Digitales
Global Commission on Stability of Cyberspace
Global Partners Digital
KICTANet
Research ICT Africa
Red en Defensa de los Derechos Digitales
Fundación Karisma
Media Foundation for West Africa