Friday, 21 July

His Excellency Ambassador Burhan Gafoor
Chair of the Open-Ended Working Group
on security of and in the use of information
and communications technologies 2021-2025
C/O The Secretariat of the OEWG
Office of Disarmament Affairs
prizeman@un.org
New York

Dear Chair,

The undersigned non-governmental stakeholders would like to thank you and your team for your work on the Second Annual Progress Report (APR) of the United Nation's second Open-Ended Working Group ("OEWG") on the security of and in the use of information and communications technologies (ICTs). Your draft provides a solid foundation upon which the OEWG can build future work. We hope to see the APR adopted during the July meeting of the OEWG and are fully committed to supporting member states in their efforts to reach a consensus.

We welcome the clear recognition in the draft APR that there is a need to connect the work of the OEWG with wider digital development efforts and the call for States to consider how potential coordination and integration with existing development programmes and funds could unlock further funding. It is vital that the OEWG leverages the wealth of existing capacity-building initiatives and draws on the experience of well-established organisations. In an increasingly digitalised world, we cannot overstate the importance of mainstreaming cybersecurity into the wider UN sustainable development agenda; there is currently a lack of alignment between the need to close digital divides and the need to improve cybersecurity. This poses a real risk to achieving an open, secure and trusted digital ecosystem. While the current draft of the APR provides a good basis, **we recommend that the APR should contain language which explicitly states that the OEWG should consider how cybersecurity considerations and good practices can be integrated into future digital development projects; while recognising the unique needs, circumstances and state of cybersecurity developments both in low and high-income countries.**

Effectively coordinated capacity building would benefit from a shared conception of what is needed to secure cyberspace, based on the existing norms of responsible state behaviour as outlined by the OEWG. We welcome the suggestion to develop a norms implementation checklist, and the intention of the Chair to produce an initial draft. At the same time, it is important to note that any such checklist must be developed in tandem with a comprehensive and coordinated approach to capacity building related to the implementation of the same norms. Without the required support to develop the technical capacities and required institutional strength to implement the framework of responsible State behaviour in the use of ICTs a checklist will remain aspirational, especially for low and middle-income countries. Further to the checklist, we hope that Member States will also consider **reflecting conversations from past meetings about the value of establishing common goals to define the scope, ambition and required capacity building support needed to implement the existing framework**.

As the APR recognises, **stakeholders are central to delivering capacity building**, and we welcome acknowledgement that they are "already playing an important role through partnerships with States for the purposes of training, research, and facilitating access to internet and digital services" but would also like

to highlight that stakeholders contribute to a wide range of other capacity building efforts. We stand ready to support States in their capacity building efforts, including on “how to identify and engage meaningfully with stakeholders in order to strengthen policy making and establish trust to cooperate with stakeholders in addressing ICT security incidents.” The proposed ‘Global Roundtable on ICT security capacity building’ provides an ideal opportunity to establish a mode of meaningful engagement, and we hope that there is an ambition for this to be a substantive and ongoing initiative involving stakeholders rather than a one-off meeting.

Finally, Excellency, we would like to underline that we stand ready to support States in their discussions on the APR and remain committed to a successful OEWG process.

Signatories:

- Africa Freedom of Information Centre
- Africa ICT Alliance
- Centre for Multilateral Affairs
- CyberPeace Institute
- Cybersecurity Tech Accord
- Derechos Digitales · América Latina
- DiploFoundation
- Global Forum for Cyber Expertise Foundation
- Global Partners Digital
- Google
- International Chamber of Commerce
- Jimson Olufuye, Kontemporary Konsulting Ltd.
- Mastercard
- Microsoft
- Northwave Cybersecurity
- Paris Peace Forum
- Professional Options, LLC
- Queue Associates, Inc.
- Red en Defensa de los Derechos Digitales, México
- Telefónica
- United States Council for International Business (USCIB)