13 December 2021

Statement on the value of multistakeholder engagement in the OEWG process (2021-2025)

The first substantive meeting of the Open-Ended Working Group[1] (OEWG) on security of and in the use of information and communications technologies (2021-2025) will take place on 13-17 December 2021. The new OEWG was established pursuant to UN General Assembly resolution 75/240, which recognizes that states "*...may decide to interact, as appropriate, with other interested parties, including businesses, non-governmental organizations and academia*…" Underscoring the importance of states engaging with the multistakeholder community, the following statement outlines substantive contributions that this community can make in support of the OEWG process.

This statement is complementary to the letter to the Chair that a group of state and non-state actors submitted earlier and that proposes a set of principles for the modalities of multistakeholder engagement that should be embodied throughout the OEWG process.

We believe an inclusive process should be promoted and maintained with regular consultative meetings. We are concerned that the Chair's letter from 15 November 2021 on the programme of work for the first substantive session of the OEWG does not address this and thus require that there is:

- specific mention of the inclusion of civil society;
- clarity on exactly how non-state actors can participate in the first substantive session;
- clarity on the level of transparency and visibility offered for multistakeholder contributions throughout the process.

Governments should ensure the inclusion of non-state actors in local, regional, and international processes. While a number of governments have reiterated their commitment towards an inclusive OEWG process in which the multistakeholder community has a voice, we believe that more clarity on potential contributions from non-state actors could encourage other governments to advocate for and pursue inclusive processes.

Our statement calls for meaningful engagement 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.

[1] An earlier process of the Open-ended working group on developments in the field of information and telecommunications in the context of international security reached consensus on its final report in March 2021.

I. Continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats.

Non-state actors can support this agenda item by providing research and operational expertise, including technical knowledge, that is global in scope. The multistakeholder community can offer:

- Extensive knowledge of the threat landscape through in-depth monitoring and provision of statistics on cyber incidents. This expertise extends to technical-level knowledge of how and why potential threats can affect critical functions in national economies and degrade public security, health and safety;
- Experience of the practical steps that organizations can take to improve their digital security and in the adoption of these steps;
- Assistance in the development and implementation of data security solutions;
- Management of initiatives for the exchange of practical information between private sector entities and with governments;
- Aid in the promotion of common understandings in the sphere of information security, and in developing a cooperative approach to counter such threats;
- Knowledge of how threats impact human rights and human security, including gender-based threats and impacts;
- Support in building sustainable and resilient communities based on experience in preventing conflict and mitigating crises in a way that promotes peace;
- Development and implementation models for cooperation between state and non-state actors for establishing processes to identify and tackle threats. Practical ideas to address this effort include effective collaboration on protecting the integrity of the supply chain and the development of a digital responsibility framework.

II. Further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour

The multistakeholder community has the capacity and knowledge to support the co-designing of the rules and principles of responsible behaviour in cyberspace. As such, non-state actors can provide guidance on the implementation of cyber norms and establish the link to a wider human rights-based framework. Based on this guidance, the community can monitor the implementation of these rules, norms and principles to foster accountability and transparency among actors. The multistakeholder community can contribute directly to:

- Awareness raising of the existing norms through partnerships and capacity building;
- Assistance in the implementation of existing norms. Research based on proximity to victims that provides clear understandings of the gaps in current norms implementation and provides recommendations to close those gaps;

- Augment states' analytical capacity regarding the potential effects that these proposed rules, norms and principles may have, including the potential interaction effects among multiple rules;
- Cooperation in the application of digital footprints to achieve better transparency for areas such as financial accountability and climate and energy tracking.

III. How international law applies to the use of information and communications technologies by States

The multistakeholder community plays a research and advocacy role in an effort to provide in-depth understanding of international law both above and below the armed attack threshold. In this way, the community enables and contributes to a rule of law ecosystem in which obligations can be enforced with the cooperation of all parties. Non-state actors are in a position to:

- Conduct analysis on the governance and accountability of state actions in cyberspace;
- Assist in the creation of tracking systems for stronger governance and oversight of digital society and digital economy that can facilitate local decision making on related matters;
- Enable shared, global learning as to how international law applies to the use of information and communications technologies;
- Provide human rights expertise on these matters and make specific contributions in regard to the human-centric approach in the application of international law.
- Contribute to the creation of remedy and compensation frameworks for victims of irresponsible behaviour in cyberspace.

IV. Confidence-building measures

The multistakeholder community drives many of the initiatives that build trust and confidence among stakeholders and encourages both state and non-state actors to make pledges on what they are doing to promote a more secure cyberspace. This work is beneficial to the OEWG process as it is based on:

- Research and monitoring of the application of confidence-building measures in different contexts;
- Field knowledge from both cyber and non-cyber domains that helps to inform local, national and regional initiatives;
- Human-centric expertise that informs confidence-building initiatives;
- Knowledge-sharing to form a repository of resilient community building journeys and narratives.

V. Capacity-building

Non-state actors use specific expertise and a needs-driven approach to work with local communities and to establish trust. They work towards an effective and sustainable capacity building process, playing a key educational role by disseminating and diffusing knowledge about cybersecurity and responsible behaviour in cyberspace. The multistakeholder community can work with states to:

- Learn more about the digital divide, disparate levels of digital literacy and cyber hygiene and how they weaken a state's national cybersecurity posture;
- Explore gaps and build inclusive solutions for individuals from communities that face digital disparity such as persons with disabilities and members of indigenous and tribal communities. This is to ensure their democratic participation and well-being in an increasingly digital world;
- Close the cybersecurity education gap with the help of non-state actors such as the civil society and grassroots groups who can work with governments and organisations on the local, national, and international level;
- Close the workforce gap, including the gender gap in cybersecurity by looking at the weaknesses in both the supply and demand side. This can include issues such as cybersecurity workforce hiring practices, the price of an education in cybersecurity and the discrimination, stereotyping, and other work-life balance considerations that typically present as barriers to those who may want to join the field;
- Operationalise principles for capacity building. In practical terms this includes: discussing what implementation of the principles looks like in practice; identifying good practice examples from what is already being done; taking into consideration lessons learned from the operationalisation of principles in other fields; and broadening and deepening regional and multistakeholder awareness and support for the principles;
- Invest in an effective building of capacities at scale.

VI. Establish, under the auspices of the United Nations, regular institutional dialogue with the broad participation of States

A coordinated approach to regular institutional dialogue should involve non-state actors so that together, we can create sustainable solutions and ensure it:

- Is action-oriented and impactful;
- Emphasizes accountability and victim redress;
- Adopts a coordinated approach to prevent cyber harm;
- Fosters transparency through inclusive dialogue to build credibility within the multistakeholder community.

This statement is supported by the following organizations:

Bangladesh NGOs Network for Radio and Communication

CCAOI

Centre for Information Technology and Development (CITAD)

CIVICUS

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Community Development Initiative

Cyber Governance and Policy Center, University of Oklahoma

CyberPeace Institute

Cybersecurity Coalition

Cyber Threat Alliance

Diplowomen

Globe International Center

Identity Valley

Indiana University Ostrom Workshop

Jokkolabs Banjul

Kenya ICT Action Network (KICTANet)

Media Development Centre Skopje

PACKS Africa

People Centered Internet

RedesAyuda

Sustainable Actions for Nature Nigeria

Swiss Digital Initiative

Women in Crisis Response (WiCR)

Yesaid Society Kenya

ZeroToOne Foundation for Youth Development

This statement remains open for additional signatories, should other organisations want to support it.