Comments from the Association for Progressive Communications (APC) on the zero draft of the report of the UN Open-ended Working Group in the field of information and telecommunications in the context of international security (OEWG)

February 2021

1. Introduction

The Association for Progressive Communications (APC) is an international organisation and a network of organisations dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communications technologies (ICTs).

APC welcomes this opportunity to address comments to the zero draft of the United Nations Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) report. We appreciate the accessibility of Ambassador Lauber to civil society and the OEWG's willingness to receive and consider comments submitted by non-state actors. APC has been following the work of the OEWG with great interest since its beginning. In

the comments below, we present some of the key issues we believe are key for an open and secure ICT environment and we make specific recommendations for consideration.

2. Preamble

APC welcomes the acknowledgement in the zero draft's introduction of the shared responsibility of non-state stakeholders in supporting a secure and stable cyberspace. We have some concerns, however, about the degree to which outreach to stakeholders has allowed for substantive participation and contribution in the process of the OEWG. While we appreciate that the consultation in December of 2019 was open to all stakeholders, we remain concerned that open participation in substantive meetings still largely excludes non-state actors, especially those without ECOSOC status.

After observing the challenge of reaching consensus on binding norms among states in the Group of Governmental Experts (GGE) efforts, we suggest that the state-centric focus of these discussions, to the exclusion of other stakeholders, has been an impediment to establishing norms rather than an advantage. The diversity of perspectives and the knowledge brought in by other stakeholders can assist states in finding a path to agreement, whether it is the gendered and human-centric views of civil society, the economic necessities from the business community, the theoretical framing from academia, or the technical realities brought by the technical community.

Recommendation: Going forward, inclusive Open-ended Working Groups should include all stakeholders.

3. Existing and potential threats

While the OEWG documents concern for the people affected by ICT disruptions, and while there is an awareness that the existing and potential threats affect different groups such as "youth, the elderly, women and men, […] vulnerable populations, particular professions, small and medium-sized enterprises, and others'' differently, these considerations should be an essential part of the ongoing process and the report could go further into this.

We emphasise again the importance of gender considerations as integral to the cyber threats discussion. Malicious cyber operations impact people differently based on their gender identity or expression. Online gender dynamics have been shown to

reinforce and amplify the social, economic, cultural and political structures and systemic biases of the offline world. As gender affects the way people and societies view the threats of weapons, war and militarism, a gender analysis of international cybersecurity would generate greater understanding of the dynamics that shape cooperative measures to address such threats.

States should work with all stakeholders to understand how vulnerable groups' enjoyment of rights is affected by cyber threats, and this should be emphasised in the OEWG report.

Recommendation: Stress the need for a human rights-based approach to understand existing and emerging threats, recognising the differentiated impacts on women and people of diverse sexualities and gender expression. Involve all stakeholders for both implementation and development of measures to address cyber threats.

4. International law

We welcome the draft's highlighting that international law is essential to maintain a secure and stable cyberspace. International human rights law should be the guiding principle to hone in on a shared, inclusive and equitable understanding of states' jurisdiction over ICT-related matters. We encourage the report to emphasise this.

However, while respect for human rights and fundamental freedoms is mentioned in the zero draft, the division between security and rights cannot be maintained when discussing the use of ICTs. Not only does the right to international security depend on the Universal Declaration of Human Rights Articles 3 and 22; international security is necessary to fulfil a state's obligation as a principle duty bearer in the guarantee of human rights as recognised by the United Nations. Protection of human rights is a security issue, and protection of those human rights online is a fundamental cybersecurity consideration.

States should comply with their international human rights obligations when designing and putting into place cybersecurity initiatives. States should refrain from the criminalisation of cybersecurity expertise and from employing unlawful or arbitrary surveillance techniques, and in line with the UN Human Rights Council resolution,[1] they should prohibit measures which intentionally prevent or disrupt

[1] https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13

access to the internet. In these considerations, the central role of the UN as a pillar of human rights, with states' responsibilities as duty bearers, should be more strongly emphasised in the zero draft.

Despite the increase in women's participation in the OEWG and progress that has been made in recognising the applicability of threats and abuses against women in digital contexts, focus on those issues remains nearly absent from consideration in the draft's discussions of the legal aspects of international peace and security and justice. The quest for international peace and security with justice should be integrated with an understanding of the effect of malicious cyber operations, by states and individuals, on people, especially those who face multiple and intersecting forms of discrimination and inequality.

Recommendation: Emphasise that protection of human rights is a security issue and that international human rights law should be a guiding principle in cyber governance. Discussions of the legal aspects of international peace and security and justice should integrate an understanding of the effect of malicious cyber operations on vulnerable groups.

5. Norms and principles for responsible state behaviour

The set of non-binding norms created by the GGE efforts and the UN General Assembly resolutions 70/237 and 73/27 have been one of the achievements of the current international cooperation. However, the norms recommendations referred to in paragraphs 47 and 60 of the zero draft would benefit from clearer guidance for operationalisation and accountability mechanisms. Without them, norms remain aspirations that have an indeterminate effect.

All relevant stakeholders, including civil society, the private sector, academia and the technical community, have a role to play in supporting states' efforts to implement the agreed-upon norms, which rely on trusted relationships, expertise, information sharing, and collaboration of all relevant stakeholders. Trust is difficult to achieve if all relevant stakeholders are not included in open, inclusive and transparent discussions on areas in which they have experience and crucial interests.

Civil society has experience working with states in monitoring United Nations system implementations. We support the OEWG recommendations for a voluntary non-binding state survey of national efforts to implement the norms. We believe,

however, that mechanisms led by states with input from relevant stakeholders, through which voluntary assessment can be made in a more consistent manner, are needed. A voluntary state-led review process, involving multistakeholder participation to facilitate the sharing of experiences, including successes, challenges and lessons learned in implementing the norms, would help in making progress in achieving the goals represented by the norms.

Recommendations: Establish mechanisms for voluntary state-led multistakeholder-facilitated reviews on norms implementation.

6. Confidence-building measures

Confidence building measures (CBMs) do not only concern states. Focusing solely on the trust between states puts people's confidence in cyber governance at risk. Principles of openness, inclusivity and transparency should apply to CBMs, as trust and confidence need to be achieved among all relevant stakeholders.

In relation to the internet, confidence, especially among vulnerable groups, can only be achieved when all stakeholders are included. Global cyber governance, including the protection of a secure and stable cyberspace, is not the work of one stakeholder group, as confidence building cuts across multiple domains and subject matter expertise. Only collectively with non-state actors can governments and multilateral forums address complex and transnational global cyber threats.

Recommendation: Adopt a multistakeholder approach for building confidence and peace and stability in cyberspace.

7. Capacity building

We welcome the credit given to non-state stakeholders in capacity building at the national, regional and international level. In developing recommendations for capacity building, open, inclusive and transparent processes that engage civil society, the private sector, academia and the technical community are essential, as they include wider perspectives and allow for sustainable outcomes. Cybersecurity 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 and economic impact and their implications for human rights.
Capacity-building efforts that emerge from the OEWG should build on existing efforts, to avoid duplication and allow synergies. These efforts should include funding for existing efforts and should avoid doing harm to existing projects and organisations.

We also value that the zero draft addresses the gender approach in capacity building as critical. While it is important that women are being included in the processes and that there is a recommendation that capacity building be gender sensitive, the gender approach goes beyond women's participation and sensitivity. Rather, gender should be mainstreamed in the design, implementation and evaluation of capacity-building programmes, and this consideration should be included within the recommendations.

Recommendation: Work with existing capacity-building efforts with a human-centric approach and integrating a gender perspective. Promote an open, inclusive and transparent approach to capacity building to include wider perspectives and allow for more sustainable outcomes.

8. Regular institutional dialogue

Given the multitude of existing programmes on cybersecurity and peace that are ongoing, both in the UN and among non-state actors, we advocate moving to a more focused set of programmes that include non-state actors in a continuing dialogue that fosters the creation of trust and a global common understanding on developments in ICTs related to international cybersecurity.

Any programme of action towards a secure and peaceful cyberspace should prioritise effective participation and inclusiveness of all relevant non-government stakeholders.

Recommendation: Include non-state actors in continuing institutional dialogue and the design and implementation of any programmes of action.