APC comments on the final report of the OEWG on cybersecurity

Association for Progressive Communications (APC)
March 2021

Background

After two years of negotiations, the Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security has adopted its final report. The OEWG, established by the UN General Assembly's First Committee in late 2018, explored the issue of responsible behaviour of states in cyberspace by discussing existing and potential cyber threats and how to address them; cyber norms, rules and principles; confidence-building measures; how international law applies to cyberspace; capacity building on cybersecurity; and the possibility of establishing regular institutional dialogue to address these issues.

APC has followed the OEWG process since its inception. From the First Substantive Session we expressed how critical it is to adopt a human rights and gender approach to cybersecurity discussions. The final report and its recommendations may end up having a significant influence on trends and policies in cybersecurity globally, with implications for human rights. Below, we present our position on some of the most salient points of the report.

The report: Salient points and APC views

The final report recognises that cyber operations and incidents may have a different impact on "different groups and entities", including youth, the elderly, women and men, and "people who are vulnerable". The report does not present recommendations on this subject, and as expressed by APC in previous comments on the draft, language here could have gone further in recognising that people's experiences

in cyberspace are not the same. The report could have, for example, emphasised the importance of gender considerations as key to discussions on cyber threats and could have offered specific recommendations to states to address this by working with other stakeholders and the groups impacted by the effects of malicious cyber operations.

The report highlights how cyber norms – such as the UN Group of Governmental Experts (GGE) norms – provide additional and specific guidance on what responsible state behaviour in the use of information and communications technologies (ICTs) entails, and reaffirms the importance of supporting and furthering efforts to implement these agreed norms at the global, regional and national levels. The report, however, could have stressed that norms should be implemented in a human-centric way. In terms of implementation, the report recommends that states use a voluntary survey to assess norms implementation at the national level. While this is important, we believe more consistent accountability mechanisms with input from all relevant stakeholders are still needed. Norms are valuable when they are actually implemented and all stakeholders play a role in contributing to this. Going forward, truly inclusive accountability mechanisms, that directly involve the actors whom the norm is intended to address, would help in making progress in achieving the goals represented by the norms.

We welcome the final report stating that international law is essential to maintain a secure and stable cyberspace and the concerns on the implications of the malicious use of ICTs for human rights. We believe the report could have given more attention to the human rights implications of cybersecurity and emphasised that cybersecurity is a human rights issue and that international human rights law should be a guiding principle in cyber governance. In the future OEWG, discussions of the legal aspects of international peace and security and justice should integrate an understanding of the effects of malicious cyber operations on vulnerable groups. Additionally, overall, the importance of a human-centric approach should be more deeply developed across discussions.

We commend the report highlighting the contribution of women delegates in the process and the importance of promoting women's meaningful participation and leadership in cybersecurity governance processes.

We also value the reference to bridging the "gender digital divide" and recommendations for cyber capacity building to be gender sensitive and inclusive. However, despite this, discussions on these issues and what states could do about them are nearly absent across the different sections of the report. We reiterate our view that gender should be mainstreamed across cyber governance discussions, from norms implementation and capacity-building initiatives to measures to address cyber threats. For this, we encourage the future OEWG to meaningfully include women's and LGBTIQ groups.

Moving forward

As we stated in our intervention during the last session of the OEWG, a much more action oriented final output would have been desirable. The report mentions the cyber Programme of Action (PoA) proposed by some states to provide more concrete recommendations to promote implementation of the existing framework and avoid duplication at the UN. The final report recommends that this PoA be further elaborated by the new OEWG that will operate for a period of five years – from 2021 to 2025 – with the same mandate.

At the OEWG, the main actors are UN member states, but there is the possibility of engagement of other stakeholders. Both the resolution that created the process and the one that renewed it explicitly mention the need for identifying mechanisms for the participation of the different stakeholders.

While we value the openness of the chair, Ambassador Lauber, to civil society participation, and the OEWG's willingness to receive and consider comments by non-state actors during informal events, the process overall lacked openness to civil society. In joint civil society statements, we expressed our regret that many of our colleagues in civil society, academia and the technical community, who do not enjoy ECOSOC status, were unable to obtain accreditation for the first substantive session of the OEWG, and in the COVID-19 context, the uncertainty and lack of information around the modalities for virtual participation worsen the situation.

Going forward, a human-centric approach to global cybersecurity, guided by principles of equity, inclusion and multistakeholder dialogue, are critical for the OEWG to actually work for a safe, open, reliable and peaceful cyberspace.