Joint civil society feedback on first draft of the OEWG on ICTs report

We, the under-signed, welcome the first substantive draft of the Open-ended Working Group (OEWG) report on ICTs and the opportunity to share our perspectives on it. In this response, we provide general feedback on each part of the report, focusing on the "introductory remarks" and the "conclusions and recommendations" sections and provide recommendations.

Overall, while we applaud the efforts of the OEWG Chair and Secretariat to involve civil society actors in the OEWG process, we think that the report does not yet reflect the importance of the multistakeholder approach to help build and maintain a secure and peaceful cyberspace, including implementing the agreed outcomes of state-led processes. Further we believe there should be greater recognition of the human impact of ICT issues, and the direct connection they have with the protection and promotion of international peace and security would strengthen the report and its role in supporting a more peaceful and secure cyberspace.

Emerging and existing threats

We welcome the references in the report to the impact of cyber operations on critical infrastructure and critical information infrastructure and their wide-ranging effects on security, economic and social development and people's well-being. However, the report does not adequately reflect the role of civil society, the technical community, academia and industry in building, maintaining and securing cyberspace. We also believe that the report should better reflect the role of States to work with affected groups to understand how vulnerable groups' enjoyment of rights is affected by the malicious use of ICTs. There is a need for greater recognition of how cyber operations impact differently in vulnerable groups in the report, as well as specific recommendations to address this, including gender-related recommendations.

Therefore, we recommend that the report:

- Reference the need for all actors to protect the basic availability and integrity of the global Internet, which includes not interfering with the public core of the Internet.[1]
- Strengthen the reference to the need to work together with other stakeholders, to understand the effect of malicious cyber operations on vulnerable groups.

International law

We welcome the reaffirmation that international law, including the UN Charter, applies in cyberspace. However, while the majority of states have reaffirmed their understanding that "international humanitarian law neither encourages militarization nor legitimizes resort to conflict in any domain", this is not reflected in the report. Furthermore, in line with our recommendation that addressing threats in cyberspace be evidence-based and handled in an inclusive manner, we recommend that the substantive part of the report references states' responsibilities regarding their use of ICTs. In particular, it should be stated that the responsibilities of States extend to

[1] As defined in https://cyberstability.org/norms/#toggle-id-1

internationally wrongful acts and that this also applies to the use of proxies, regardless of whether they take place on a state's territory or not.

Therefore, we recommend that the report:

- Include reference to international law in its entirety, including international humanitarian law and international human rights law, applies in cyberspace.
- Strongly encourage states to inform the UN Secretary-General of their national views and practices for his annual report on ICTs.
- Include reference to State's responsibilities for failure to act when they knowingly allow their territory to be used by other actors for acts contrary to other States' rights, including through the use of proxies.

Rules, Norms and Principles

We welcome the reference to the non-paper in the recommendations section and the guidance provided for the implementation of norms. However, the implementation of norms should be an inclusive effort and in particular should directly involve those actors whom the norm is intended to address. It should be implemented in a human-centric way if they are to impact international peace and security positively. This is not yet referenced in the report.

Therefore, we recommend that the report:

- Recommend states to work together with other stakeholders, including civil society, technical community, academia and industry to develop new norms and to implement the agreed norms, and should suggest that states share practices and examples on engaging with stakeholders in a standard and regular way with regards to cyber norms implementation.

Capacity building

We welcome the reference to non-State stakeholders in capacity building and the principles, particularly those that state that capacity building efforts should respect human rights and be non-discriminatory, as well as inter-regional and cross-regional exchanges. We also welcome the reference to the need for a gender-sensitive approach, but believe this needs to be strengthened. There is also a need to recognise that in a world increasingly dependent on digital technologies, the cyber capacity building agenda must align with the broader development agenda.

Therefore, we recommend that the report:

- Recognise the need for greater resources to be made available for capacity building efforts, by directly referring to this in the recommendations section.
- Recognise the need for gender considerations to be mainstreamed in designing, implementing and evaluating capacity building programs.
- Support the alignment or integration of capacity building into the implementation of the broader sustainable development agenda.

Regular institutional dialogue

We welcome the report's recognition that any future mechanism for regular institutional dialogue should be an action-oriented process, building on previous outcomes, and should be inclusive, transparent, consensus driven and results-based. However, any mechanism must be inclusive not just of States but also of all stakeholders, including civil society, the technical community and academia. There are a variety of lessons learned that States can consult and integrate from other forums in this regard. We also welcome the reference to the Programme of Action in the recommendations section of the report. Still, we believe that this reference should also include the need for institutionalised consultation and engagement with all stakeholders, not just States (as it is currently worded) to strengthen and enhance collective action/cooperation in safeguarding the peace and stability of cyberspace.

Therefore, we recommend that the report:

- Refer to the need to engage other stakeholders in a meaningful way, including applying lessons learned from other relevant forums and processes, in any future regular institutional dialogue.

Confidence-building measures (CBMs)

We welcome the report's reference to the importance of CBMs and their link with norms in fostering trust and ensuring greater clarity, predictability and stability in the use of ICTs among States. We also welcome the reference to the need for transparency measures, but suggest this should be extended. States should be encouraged to take more measures to be transparent about their behaviour. This would help understand the motivations behind certain actions and developments and build trust among State and non-State actors.

The report recognises that there are various multi-stakeholders' initiatives that exist to contribute to CBMs, but the text makes no direct reference to non-governmental stakeholders who are actively involved in the discussions on how to implement CBMs effectively. Non-governmental stakeholders can play key roles in capacity building, as well as in the design, implementation, monitoring and evaluation of CBMs. Underrepresentation of the work of civil society groups and other multistakeholder initiatives can lead to a myopic assessment of gaps and effective planning CBMs.

Recommendations

- Encourage States and Regional Organisations to be more transparent about their implementation of CBMs.
- Encourage States to work with other stakeholders to support more effective implementation of CBMs.
- Encourage States to undertake concrete steps towards developing and implementing standard CBMs to support active progress on their implementation.

SIGNATORIES

Access Now
Association for Progressive Communications (APC)
Global Commission on the Stability of Cyberspace / The Hague Center for Strategic Studies
Global Partners Digital (GPD)
Jokkolabs Banjul, The Gambia
Kenya ICT Action Network (KICTANet)
Igarape Institute
Media Foundation for West Africa (MFWA)
Research ICT Africa