Zero-draft of the OEWG's report on ICTs

GLOBAL PARTNERS DIGITAL

Global Partners Digital response

February 2021

About Global Partners Digital

The advent of the internet – and the wider digital environment – has enabled new forms of free expression, organisation and association, provided unprecedented access to information and ideas, and catalysed rapid economic and social development. It has also facilitated new forms of repression and violation of human rights, and intensified existing inequalities.
Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values. We do this by making policy spaces and processes more open, inclusive and transparent, and by facilitating strategic, informed and coordinated engagement in these processes by public interest actors.

Our submission/output

GPD welcomes the Zero Draft of the Open-ended Working Group (OEWG) report on ICTs and the opportunity to share our perspective on it.

As with our response to the initial pre-draft of the OEWG report, central to our input are two key points:

1. Discussions relating to peace and security in cyberspace—and what is permissible and impermissible behaviour in cyberspace—are directly tied to and impact human rights;
2. Due to the characteristics of ICTs as primarily civilian technologies, which were developed and continue to evolve due to the critical involvement of non-state actors, the maintenance of international peace and security in cyberspace must be an effort inclusive of all stakeholders

In this response, we provide feedback pertaining to each section of the zero-draft of the report, including specific recommendations.

Preamble

GPD welcomes the references included to human rights and the human centric approach and strongly supports the inclusion of these references. However, in order to support greater understandings of the term, we encourage member states to elaborate their perspectives and understandings of 'human-centric', including by sharing examples. Each element of the OEWG's mandate (existing and emerging threats; rules, norms and principles; international law;) can and should be interpreted in a human-centric manner. Negative trends in the digital domain could undermine international security and stability, economic growth and sustainable development, and hinder the full enjoyment of human rights and fundamental freedoms.

Existing and Emerging threats

GPD welcomes the recognition that threats are perceived differently by different actors and that they may be experienced differently by both states and on different groups and entities. However, the report should also recognise that addressing these threats should be done in consultation with all stakeholders. In the section on existing and emerging threats, the report should emphasise the role of different actors in addressing cyberthreats, and underscore the importance of taking special steps to involve stakeholders who are more vulnerable to cyber threats, including civil society organisations and marginalised communities in developing responses to address these threats. In addition, there are references to the OEWG format which may be misleading (see page 3). The OEWG format was not inclusive of all stakeholders and a number of delegations have repeatedly raised this concern.

Recommendations

- Include references in the text to the role of different actors in addressing cyberthreats
- Underscore the importance of involving stakeholders who are more vulnerable to cyber threats, including civil society organisations and marginalised communities, in developing responses
- Underscore the importance of a human-centric approach to addressing cyberthreats including through a focus on the impact of malicious cyber operations on people and communities

Rules, norms and principles

GPD welcomes the report's assessment that the norms be viewed as consistent with international law and with the purposes and principles of the United Nations, including to maintain international peace and security and the promotion of human rights. However, as the report does in the section on "confidence-building measures", references should also be made to the work done in relevant forums, including those related to the UN, which can support the implementation of the agreed 11 GGE norms. For example, work done by the multistakeholder community within the framework of the Internet Governance Forum has identified a range of good practices and challenges to norm implementation.

Currently the report states that non-governmental stakeholders should "uphold their responsibilities" in their use of ICTs. However, we believe this should be further explained, or complemented by a recognition that with regards to norms, it is states who have committed to certain actions and measures through the norms adopted in 2015, and have responsibilities to uphold them. In order to effectively implement the norms and uphold their responsibilities, they should cooperate with other stakeholders. During the course of the OEWG discussions, States have repeatedly recognised the importance of engaging non-governmental stakeholders, including civil society, the technical community and industry in a peaceful and secure cyberspace. This cooperation is also relevant to the implementation of norms. Civil society, for example, includes their role in raising awareness and socialising the norms, capacity building, monitoring implementation, providing evidence-based research, and proposing specific technical and policy solutions to implement the norms.

GPD supports the development of guidance for the implementation of norms and believes that the discussions have reflected the need for that. Therefore, GPD supports the reference to the non-paper as an annex.

Recommendations

- This section should include a recommendation that states, in consultation with other stakeholders, including civil society, to identify the relevant frameworks, such as national cybersecurity strategies and policies, where the norms can be operationalised at the national and regional levels.
- The report mentions norm implementation (paragraph 49) but does not mention the need to engage with all stakeholders in norm implementation. It should explicitly recognise the role of civil society in norm implementation. States implement agreed cybernorms in cooperation with non-governmental stakeholders, including civil society, the technical community and industry.
- The report should make reference to engagement with other relevant initiatives, including multistakeholder initiatives.

International law

GPD welcomes the reaffirmation that international law—particularly the UN Charter—is applicable and essential to maintaining peace and stability (paragraph 27) and that international law can develop progressively, including through opinio juris and State practice.

As noted in Paragraph 31, challenges remain with regards to accountability and transparency for state actions in cyberspace. This should be strengthened to refer to, for example, in attributing internationally wrongful acts, guidance could recommend that any verification mechanisms should be strong, impartial and verifiable and should involve other non-governmental stakeholders, so as to build trust and confidence. This will also support the application of international law in cyberspace.

In addition, GPD agrees that there is a need for more States to publish their positions on how international law, including international human rights law, applies in cyberspace and a need for greater capacity building to support the development of these positions. As well as states, other stakeholder groups can also play a role in helping understand how international law applies in cyberspace. The report should recommend that states consider national-level consultation processes in order to engage with non-governmental stakeholders when developing their own positions, as well as drawing upon the expertise that exists among non-governmental stakeholders as part of their own capacity-building efforts.

Recommendations

- Strengthen the call for states to share their views on how international law applies in cyberspace, for example by "strongly encouraging" states to submit their views to the UN Secretary General's annual report.
- Make it clear in the "Conclusions and Recommendations section" that international law in its entirety applies to cyberspace.
- Include the obligations enumerated in paragraph 28-30 in the "Conclusions and Recommendations section".
- References to international law should also refer to international human rights law, which applies at all times, including in peacetime.

Confidence-building measures

GPD welcomes the report's recognition that the implementation of CBMs can strengthen the overall security, resilience and peaceful use of ICTs, as well as the recognition that a variety of multistakeholder initiatives exist and have contributed to confidence building. However, there is a need for greater transparency and information sharing on the implementation of CBMs - in order to assess and monitor their effectiveness and contribute to better implementation. A role can also be played here by other stakeholders including civil society, technical community, academia and industry and this should be referenced in the report.

Recommendations

- The CBM recommendations should include a recommendation that states work with other stakeholders on their implementation.
- The report should recommend greater transparency and information-sharing regarding the implementation of CBMs.

Capacity building

GPD agrees that capacity-building is a shared responsibility as well as a reciprocal endeavour, and welcomes the reference need for capacity building to respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory. GPD also welcomes the recognition that sustainability in capacity-building can be enhanced by an approach that entails engagement and partnership with local civil society, the technical community, academic institutions and private sector actors. However, this is not reflected in the conclusions and recommendations.

Recommendations

- Reference to the need to engage all stakeholders, including civil society, in the development and implementation of capacity building efforts is included as a specific recommendation.

Regular institutional dialogue

GPD agrees that "a wider community of actors is ready to leverage its expertise to support States in their objective to ensure an open, secure, stable, accessible and peaceful ICT environment.". However, we believe that the report misleadingly notes that there "has been broad engagement with other stakeholders". The report should note that there have been significant challenges to non-governmental stakeholder engagement throughout the course of the OEWG discussions, a situation which was exacerbated by the COVID-19 pandemic.

Therefore, this should be strengthened to include reference to the need for inclusive dialogue with non-governmental stakeholders, for example by stating a peaceful and secure cyberspace requires meaningful engagement with other stakeholders. Many states have expressed the views that there is a need for this dialogue. We believe that the proposal for a Programme of Action, dependent on meaningful and inclusive mechanisms for civil society participation, could support the widely recognised need among both States and non-governmental stakeholders for and the implementation of existing commitments and recommendations, including developing guidance to support and monitor their implementation; coordinating and strengthening the effectiveness of capacity-building; and identifying and exchanging good practices.

However, there is a wide range of learnings that can and should be leveraged from other forums, including the implementation of other Programmes of Action in order to ensure meaningful inclusivity in any future regular institutional dialogue. This includes modalities that enable stakeholders to engage in real-time, side events or expert panels agreement on standing rules for participation as part of rules of procedure. The report should make reference to the need to engage with stakeholders to apply lessons learned from these forums.

Recommendations

- The report should note that there were significant challenges to non-governmental stakeholder engagement throughout the course of the OEWG discussions, a situation which was exacerbated by the COVID-19 pandemic
- The report should encourage States to engage other stakeholders in identifying and incorporating lessons learned on meaningful stakeholder engagement from other forums, including Programmes of Action.