Civil society perspectives on the “Initial pre-draft of the OEWG on developments in the field of information and telecommunications in the context of international security”

We, the under-signed, welcome the Initial Pre-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 feedback on the narrative and descriptive parts of the pre-draft, namely sections A-G. We also respond to recommendations in section H, and where relevant suggest additional recommendations.

Comments and recommendations on sections A-G

We strongly support the following elements of the report:

- We agree that new threats should be addressed through “"a framework of international law, voluntary norms and confidence building measures" (paragraph 5) and we reiterate that applicable international law includes international human rights law, as well as international humanitarian law.
- We strongly support the key principles "inclusivity, transparency and trust" (paragraph 7).
- We believe the idea of sharing best practices should be encouraged and emphasised (paragraph 37).
- We agree that cooperation among CERTS, national point of contacts, repositories (of CBMs) and universalisation of best regional practices should be supported (paragraph 42).
- We believe civil society has a role to play in contributing to "building trust and confidence in the use of ICTs" and this should be strongly emphasised in the report (paragraph 47)
- We support efforts to link cybersecurity to the Sustainable Development Agenda (paragraph 48).

We suggest the report could be strengthened in the following ways:

We support the importance the report gives to the need to narrow the “gender digital divide” and of promoting effective and meaningful participation of women in these processes (paragraph 9). We also encourage the report to address the gender dimensions of cybersecurity. It is critical to recognize how cyber threats affect differentially groups in positions of marginalization or vulnerability because of their sexual orientation or gender identity.

We support the human-centric approach proposed by the pre-draft. We encourage the report to further develop understandings of this term, or to encourage member states to elaborate their perspectives and understandings of the term, including by sharing examples. We recommend that a description of 'human-centric' include specific reference to this approach as one that puts people at the center and ensures that trust and security in networks and devices reinforce human security. A human-centric approach should be grounded in human rights and should address the technological, social, and legal aspects systematically.

We support the references to involving other stakeholders (paragraphs 7, 40, 64 and 66) but strongly recommend that this is further strengthened by referring to the wide roles played by non-government stakeholders. This includes civil society, technical community and industry - all of whom play a very wide range of roles in protecting a secure and stable cyberspace, including but not limited to the development and implementation of policy and technical security standards, carrying out research and monitoring implementation of standards..

We are concerned about the increasing use of cyberspace for offensive purposes, sometimes referred to as "militarization" of cyberspace. It is important that the discussions in the OEWG refer to and reflect relevant discussions elsewhere in the UN First Committee, including in the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (*GGE LAWS*).

We agree with the statement that a "lack of awareness, resilience and adequate capacities constitute a threat in itself" (paragraph 16). However, the report should also refer to the role of civil society in addressing this threat, particularly with regards to awareness raising and capacity building.

We agree that the differential impact of threats is important to recognise and should be emphasised (paragraph 17). Therefore vulnerable groups and civil society should be consulted in developing responses to address these threats and the report should reflect that.

We agree that responsible reporting on vulnerabilities is important (paragraph 38). We also recommend that references are made to the importance of reporting data breaches in an open, inclusive and transparent manner. There should be transparency with regards to recording of cyberattacks, cyberthreats including vulnerabilities and engaging all relevant stakeholders in reporting and monitoring.

Attacks on critical infrastructure, and here also on "supranational critical information infrastructure" (which should be understood to include the Domain Name System and other elements of the public core of the Internet), pose not only "a threat to security but also to economic development and people's livelihoods" (paragraph 19). We suggest that this human cost of attacks on critical infrastructure and their impact on human rights be directly and clearly referred to in the report.

We recommend that measures to promote responsible State behaviour remain technology-neutral and focus on actor behaviour, as opposed to the technology itself. Where references to encryption and other security-enhancing technical measures are made, the report should acknowledge the key role of encryption as a tool that allows availability, integrity, and confidentiality of the internet and which allow for the exercise of human rights through ICTs.

We believe references to international human rights and international humanitarian law are essential and must be seen as an integral part of the "framework of international law, voluntary norms and confidence building measures" (paragraph 5). A politically binding commitment with regular meetings would need to be inclusive of all stakeholders, periodic reporting, and include clear priority for human rights. It is important for any approaches to be flexible and issues-based and to support other relevant bodies, including regional mechanisms to engage.

We support the language around the value of international humanitarian in itself, and recognising that “international humanitarian law neither encourages militarization nor legitimizes conflict in any domain” (paragraph 25). We believe that the recognition that international humanitarian law “reduces risks and potential harm to both civilians and combatants in the context of an armed conflict” helps reiterate the important principle around the essential importance of protecting civilians in the unfortunate event that armed conflict involving ICT attacks does take place.

We have concerns regarding the equation of ICT attacks with acts of war that could trigger Article 51 (paragraph 27). We believe the report should be unequivocal about the applicability of all bodies of international law, including international humanitarian law to cyberspace. We have concerns that an ICT attack should not be taken lightly as an ‘armed attack’ triggering Article 51, because only the ‘most grave forms of the use of force’ constitute such armed attacks” under international law - including the opinions of the International Court of Justice. We recommend that the report refer to the report of the International Committee of the Red Cross on the “The potential human cost of cyber operations”.

We support efforts to innovate mechanisms for dispute resolution and technical attribution. However, technical attribution efforts should support a multistakeholder approach which engages all relevant stakeholders to build strong, impartial and verifiable verification mechanisms that build trust and confidence.

We support the recommendation in paragraph 38 that the general availability or integrity of the public core of the Internet should be protected, which should be understood as further specification or elaboration of the already agreed 2015 GGE norms to protect critical infrastructure. Public core refers to critical elements of the infrastructure of the Internet, namely packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centers.

Overall, we believe that references to other stakeholders should reference meaningful engagement with civil society, academia, and the technical community in the development and implementation of measures to address threats and improve security, from a human-centric lens. References to engagement with non-government stakeholders should be more detailed, strengthened and should include specific reference to the importance of engagement underpinned by openness, inclusivity and transparency principles. There is a need to provide clarity on engagement opportunities early on and have access to all relevant documentation.

We recommend that the section on capacity building refers clearly to different aspects and elements of capacity building, including the need for capacity building efforts to address gaps in both technical and policy capacity among all stakeholders, and to involve all stakeholders in addressing those gaps.

We suggest "guiding principles" for capacity building measures include the need for capacity building to be "human centered" or "human centric" and holistic.

We strongly support South-South cooperation, the multistakeholder model, and efforts to overcome the "gender digital divide" and digital inequalities more broadly. However, the report should also emphasise the need for North-South cooperation beyond donor-recipient relationships. New forms of cooperation should be rather underpinned by collaboration.

We agree that established venues within the UN (paragraph 60) may not be a substitute for the need to have a "regular dialogue". However, regular institutional intergovernmental dialogue requires an innovative involvement of non-state actors. This should include opportunities for meaningful engagement with non-governmental organisations. Broad-based formats such as the "Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2-4 December 2019)" should be further encouraged, with an emphasis on *formalising* such multistakeholder meetings with non-state actors. Full support for "national multi-stakeholder consultations" should also be referred to and references made to multi-stakeholder processes and forums, such as the global Internet Governance Forum and its Best Practice Forum on Cybersecurity, and national and regional IGFs.

We encourage the report to explicitly express that States are also responsible for respecting, fulfilling and protecting human rights in the governance of cyberspace.

We recommend that the final OEWG report refers to the report of the "Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2-4 December 2019)" and that the report be annexed to OEWG's report. It should request that member states also take note of the report of the "informal intersessional".

Comments and recommendations on section H

We provide recommendations below on how the existing recommendations in the report could be further strengthened. In addition, we provide proposals for further recommendations which could be included in the report.

International law

1. The report should acknowledge the responsibility of the private sector regarding human rights, by referring to the UN Guiding Principles on Business and Human Rights.
2. The report should highlight that international law provides the framework for restricting the sale of technologies that are used for malicious attacks.
3. We welcome the draft highlighting that secure and stable cyberspace must be grounded in both international human rights law and international humanitarian law (Para. 22). The report should request states to explicitly refer to and build on the work of UN bodies and Special Procedures on how international human rights law applies in digital contexts[1], adding guidance on the safeguarding of the right to privacy[2], freedom of expression[3], freedom of peaceful assembly and of association[4], and on violence against women[5].
4. Important to protect fundamental human rights when developing and implementing cybersecurity laws and strategies
5. We support the recommendation that States should share their views on how international law applies in cyberspace both to the Secretary General and the UNIDIR portal. We additionally recommend that states specifically include their views on how human rights and fundamental freedoms apply in this context. Human rights considerations are taken into account by states as they develop national views as it will help address the underlying conditions that lead to global insecurity.
6. We recommend that the report request states to support inclusive, transparent and multistakeholder attribution efforts that build trust and confidence.

Norms, rules and principles

7. We recommend that call for gender to be mainstreamed in both the elaboration and the implementation of norms
8. We recommend that the report call for human rights to be mainstreamed in the elaboration and implementation of norms

---

[1] Resolution of the Human Rights Council on "The promotion, protection and enjoyment of human rights on the Internet" A/HRC/38/L.10/Rev.1

[2] https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx

[3] https://www.ohchr.org/en/issues/freedomopinion/pages/opinionindex.aspx

[4] https://www.ohchr.org/EN/Issues/AssemblyAssociation/Pages/SRFreedomAssemblyAssociationIndex.aspx

[5] https://www.ohchr.org/en/issues/women/srwomen/pages/srwomenindex.aspx

9. We recommend the OEWG call for the establishment of an information sharing mechanism to support the implementation of the 11 GGE norms. Assessments of norm implementation should be periodic and publicly available. Any mechanism should include meaningful opportunities for non-government stakeholders and regional bodies to participate. We acknowledge the Mexico and Australia proposal in the non-paper. However, we believe it could be further strengthened by referring to the need for NGOs to input, including via exchange of views between OEWG delegates and NGOs, and the opportunity for NGOs to contribute written input.
10. We recommend that the report call on states to support capacity building efforts to support the implementation of norms

CBMs

11. We recommend that the role of non-governmental stakeholders, including civil society and the technical community in both developing, implementing and monitoring the efficacy of CBMs be emphasised.
12. We recommend CBMs be discussed at both multilateral and multi-stakeholder forums and processes in an inclusive and transparent manner.

Capacity building

13. We recommend that the principles of openness, inclusivity, transparency, and a multistakeholder and multidisciplinary approach underpin capacity building efforts
14. We recommend that the report recognise the need for all capacity building efforts to be underpinned by a human-centred approach
15. Need for capacity building support to implement international law
16. We recommend that the States consider support and engagement with the UN's Technology Facilitation Mechanism,
17. We recommend the report to explicitly recognize the need to build capacity also in human rights law and its application in cyberspace.

Regular institutional dialogue

18. A continuation of the OEWG or any regular institutional dialogue should ensure greater inclusivity and develop meaningful mechanisms for engagement with a wide range of stakeholders, including non ECOSOC NGOs and place particular emphasis on the need for measures to be taken to support the role of civil society and the technical community.
19. We recommend that the report of the Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2-4 December 2019) is annexed to the OEWG report
20. We recommend that the report emphasise the importance of "bottom-up" approaches to engagement with national stakeholders, and the development and utilisation of national consultation mechanisms which are open, inclusive and transparent.

Supporters

Access Now
Association for Progressive Communications
Centre for Communication Governance at National Law University Delhi
Derechos Digitales
Fundación Karisma
Global Partners Digital
Kenya ICT Action Network (KICTANet)
International Center for Not-for-Profit Law
R3D: Red en Defensa de los Derechos Digitales
Research ICT Africa
Media Foundation for West Africa
YMCA computer training centre and digital studio, the Gambia