Joint civil society input to the revised zero draft of the second annual progress report of the OEWG 2021-2025

Published 24 July 2023

A. Overview

- Paragraph 5: We welcome reference to engaging stakeholders in a "systemic, sustained and substantive manner" and the inclusion of "businesses, non-governmental organisations and academia".
- Paragraph 6: We welcome recognition of the role of regional and sub-regional organisations in implementing the framework for responsible state behaviour.
- Paragraph 7: We commend the recognition of women delegates' active participation in the sessions and the prominence given to a gender perspective during the discussions. This emphasis is essential to fostering inclusive and diverse approaches to addressing international cybersecurity challenges. We support the report's recognition of the importance of narrowing the "gender digital divide". We also value the acknowledgment of the importance of promoting women's full, equal, and meaningful participation and leadership in decision-making processes related to the use of ICTs in the context of international security. We also encourage members of the group to recognise the need to address the lack of intersectional diversity in cyber policy decision-making spaces. Recognising this would be a positive step towards building more inclusive and representative discussions and decisions.

B. Existing and Potential Threats

- Paragraph 15: We support the proposal to develop a repository of threats to ICT security while noting that the technical community, specifically vulnerability researchers, businesses, non-governmental organisations and academia, play a vital role in detecting and monitoring threats. For example, civil society organisations have detected and documented the use of malware and spyware and identified the absence of basic security protocols in state webpages and systems. **We recommend that paragraph 15 reflects that non-governmental stakeholders should be able to receive information about states' contributions to the repository and assess the information shared and ensure it is objective and evidence-based.**
- Paragraph 16: We welcome the reference to the "need for a gender perspective in addressing ICT threats and to the specific risks faced by vulnerable groups" as well as to the need to address growing digital divides. We encourage the group to delve deeper into the concept of integrating a gender perspective in addressing cyber threats and to explore the measures that States can undertake to effectively implement such an approach. For example, the framework published

by the Association for Progressive Communications (APC)[1] provides recommendations to map and understand the differentiated risks and impacts of cyber threats so cybersecurity can be tailored to address complex and diverse needs, priorities, and perceptions based on gender and other factors.

- We also consider it important to specify in the report those groups which face elevated and particular risks in the digital environment—including women, LGBT+ communities, racialised groups, people in the Global South and those in vulnerable professions (e.g. activists and security researchers). **We recommend that paragraph 16 recognises the differentiated risks and impacts of ICT threats on a wider range of groups.**
- We further urge that the report broadens its scope to not only focus on high-level state-sponsored attacks and recommends that states account for the most persistent and grave harms against people. For example, those in vulnerable professions face threats such as illegal surveillance using spyware, Open Source Intelligent (OSINT) software, malware, and biometric identification systems from malicious actors. In addition, attacks on critical electoral infrastructure and malware used to collect voters' information can influence or subvert democratic processes and undermine individuals' rights to free and fair elections, privacy and freedom of expression. **We also recommend that paragraph 16 recognises a broader range of ICT threats.**
- Paragraph 21: When considering relevant experts, it is important to recall the vital role of a diversity of stakeholders in exchanging views and acquiring knowledge about potential threats. It is particularly important to consider the role of the most impacted groups in identifying potential threats and contributing to policy solutions to address and remedy their impacts. Their perspectives should be meaningfully taken into account and should guide the development and implementation of relevant laws, norms and standards. **We recommend that paragraph 21 explicitly endorses a broad range of non-governmental stakeholders.**

C. Rules, Norms and Principles of Responsible State Behaviour

- Paragraphs 22-23: We welcome that sub-paragraph 22(c) encourages states to work with the private sector and civil society to improve security in the use of ICTs. **However, we advise that paragraphs 22 and 23 are revised to acknowledge the role of all relevant stakeholders in developing a common understanding of and facilitating the implementation of the 11 specific voluntary, non-binding norms for responsible state behaviour.**
- Civil society organisations play a vital role in ensuring evidence-based, human-centric and rights-respecting approaches to norm implementation. They have helped to foster a common understanding of the norms by developing working

[1] APC, "A framework for developing gender-responsive cybersecurity policy", 2023, available at: https://www.apc.org/en/pubs/framework-gender-cybersec.

papers, guidance and checklists to further understanding of key terms, and contextualising the norms in their national and local contexts, which should be reflected in paragraphs 22-26. This is critical because "cyber norms are derived from and refer to international law, which includes international human rights law, and require states to respect their obligations under them".[2]

- Paragraph 22: We welcome the detailed discussions of norms f, g and h, but recommend that further attention is given to norm e, which requires that states ensure the secure use of ICTs in accordance with Human Rights Council resolutions on the promotion, protection and enjoyment of human rights, including the right to privacy. There is a need to further develop an understanding of its scope and ensure its implementation, including by considering potential ramifications or consequences for non-compliance. **We recommend that paragraph 22 is amended to expressly encourage states to expand on their implementation and understanding of norm e.**
- Paragraph 26: Specifically, norm implementation guidance should recognise the need for cooperation with different non-governmental stakeholders, including civil society, the technical community, academia and private industry. **We recommend that paragraph 26 explicitly recognises the need for cooperation with non-government stakeholders in developing norm implementing guidance.**
- Paragraph 27: Any informal intersessional meeting should include all relevant stakeholders and provide space for discussions and the sharing of best practices, and we applaud that this paragraph encourages the Chair to include a range of relevant stakeholders in these discussions. We recommend that the implementation of existing norms and possible clarification or development of additional norms in a human-centric, rights-promoting and gender-sensitive manner is a key focus of these discussions.

D. International Law

- Paragraph 28: We are pleased that the revised paragraph reaffirms the recommendation of the first APR of this OEWG (2022) that states progress discussions on topics including human rights and fundamental freedoms. This reflects the substantive and intersessional discussions, where the application of international human rights law has consistently been raised by member states and stakeholders, as well as the references to it in the most recent UN GGE and OEWG reports. International law and its various branches create an overlapping and protective framework for how states should interact with one another, which is essential to maintaining peace and stability in cyberspace. We additionally welcome that this paragraph reaffirms the application of international humanitarian law in the cyber context with reference to the 2021 and 2015 GGE

[2] APC, Global Partners Digital, "Unpacking the GGE's framework on responsible state behaviour: Cyber norms", December 2019, available at: unpacking_gge_cyber-norms.pdf (gp-digital.org).

reports. This accurately reflects the consensus among states that international humanitarian law is applicable to cyber operations.[3]

- Paragraph 30: We agree that there is a need to foster common understanding on the topic of international law, and consider that states should be more strongly encouraged to share their national and regional views as a way of identifying where consensus exists as well as varying approaches to particular issues.
- Paragraphs 31-34: **The recommendations in paragraphs 31-34 should refer to the role of non-governmental stakeholders in fostering a common understanding of how international law applies in cyberspace.**
- Paragraph 32: **Specifically, we recommend that paragraph 32 explicitly encourages states to engage with non-government stakeholders when developing national positions on international law**. Non-governmental stakeholders have a vital role to play in this regard, to provide one example of such assistance: Global Partners Digital published a guide to assist civil society and government actors to assess state positions on the application of international law in cyberspace from a human-centric and rights-promoting perspective.[4]
- Paragraph 32: We support the development of a tracker of state positions. We recommend that any tracker builds upon existing initiatives,[5] and is presented in a way which enables comparative analysis and monitoring of patterns of consensus and convergence in state positions.
- Paragraph 33: We welcome the proposal to convene a dedicated intersessional meeting on how international law applies in cyberspace and recommend that it includes a discussion of the application of international human rights law and international humanitarian law. **We recommend that paragraph 33 reflects that expert briefings should be inclusive of and allow for the participation of non-governmental experts.**
- Paragraph 34: This paragraph should reflect the important role of all relevant stakeholders in enhancing capacity sharing on international law, including by assessing state positions, submitting expert opinions on the international law implications that different cybersecurity state policies could have, and contributing their expertise to ensure relevant laws, standards and policies are consistent with obligations under international human rights law. **We recommend including an explicit acknowledgement in paragraph 34 of the role of relevant non-governmental stakeholders in enhancing capacity on international law.**

---

[3] Michael Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace", Just Security (2021); and Adina Ponta, "Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes", ASIL Insight, 30 July 2021.

[4] Global Partners Digital, "Application of International Law in Cyberspace: Human Rights Assessment Guide", March 2023, available at: Application-of-Intl-Law-in-Cyberspace-Human-Rights-Assessment-Tool_GPD_.pdf (gp-digital.org).

[5] See, The Cyber Law Toolkit, available at: International cyber law: interactive toolkit (ccdcoe.org).

E. Confidence-Building Measures

- Paragraphs 36-39: **We welcome the progress made in consolidating the Points of Contact Directory (PoC Directory) and strongly advise that the establishment of further substantive standards is added to the recommended next steps in paragraphs 36-39**. These standards should include rules for designating the national agency that will become the point of contact, given the reality that some states do not have a national cybersecurity institution and that it is therefore unclear which institutions would be the most appropriate to designate; and the development of basic standards that such agencies must fulfil to be assigned this mandate, including data protection standards and respect for human rights. The designation of a national agency as a point of contact should also require that the proposed agency follow standards, including transparency, working openly with stakeholders, conducting evidence-based work and complying with human rights obligations. We recommend that such standards are included as part of the recommended next steps.
- Paragraph 35: We welcome that sub-paragraph 35(e) encourages engagement with regional and sub-regional organisations and interested stakeholders. We advise that there is also a need to create a point of contact between the PoC Directory and international CERTs in businesses and non-governmental organisations, such as the Computer Incident Response Center for the Civil Society (CiviCERT), also be reflected.

F. Capacity-Building

- Paragraph 40: We welcome the acknowledgement in sub-paragraph 40(g) of the role of stakeholders in "training, research and facilitating access to the internet and digital services" and of meaningful stakeholder engagement as a capacity-building measure to strengthen policy-making and address ICT security incidents. **We recommend the language in paragraph 40 be strengthened by recognising that stakeholders contribute "<u>to a wide range of capacity building efforts, including</u> training, research and facilitating access…".**
- Paragraphs 41-48: We advise that paragraphs 41-48 be amended to better reflect the expertise of non-governmental stakeholders in conducting and enhancing capacity building and the added value of multi-stakeholder dialogue in achieving cyber capacity building outcomes.
- Paragraph 45: We welcome the encouragement in paragraph 45 to include all interested stakeholders in the proposed roundtable on ICT security capacity-building. Non-governmental stakeholders enhance and undertake capacity building efforts in multiple ways: for example, they can contribute by working directly with the most impacted groups; developing human-centric and rights-respecting policy solutions to aid the implementation of the agreed framework; and connecting cyber capacity building to development agendas.

- Paragraphs 40 and 47: We applaud the references in paragraphs 40 and 47 to promoting "gender-sensitive" capacity-building and to the development and sharing of tools to assist states to integrate a gender perspective. A gender-sensitive approach to cyber capacity building acknowledges and addresses the varying cyber and critical tech access, opportunities, resources, benefits, and risks experienced by women, LGBTQI+ individuals, and gender-diverse people. It avoids assuming uniform needs, priorities, and capacities in relation to cybersecurity.[6] **We further recommend that paragraphs 40 and 47 refer to the role of groups facing elevated and specific risks in the digital environment—specifically women and people of diverse sexualities, gender expressions, and identities—in contributing to the design, implementation and evaluation of capacity-building measures, and specifically to the design of tools to facilitate states to promote a gender perspective.**
- Paragraph 47: We welcome that this paragraph refers to mainstreaming the capacity-building principles from the 2021 OEWG report. **We recommend that paragraph 47 directly references that capacity-building should "respect human rights and fundamental freedoms, be gender-sensitive, inclusive, universal and non-discriminatory."**[7] We also recommend that, in the development and sharing of tools, existing initiatives and collaboration among stakeholders across regions be encouraged.
- Paragraph 48: We welcome the reference in this paragraph and throughout the report to regionally-focused cooperation. The Association for Progressive Communications (APC) and Global Partners Digital's experience of facilitating the African School of Internet Governance (AfrISIG) 2022 showcased the utility of regional capacity-building and of regional, multi-stakeholder dialogues in positively shaping global cyber discussions. Another example of cooperation in capacity building is the continuous work between Fundación Karisma (Karisma) and the Colombian government in the development of the disclosure of vulnerabilities policy: Karisma has been presenting vulnerability reports, providing good practices for the design of the policy, and building bridges between the state and cybersecurity experts.

G. Regular Institutional Dialogue

- Paragraph 49: Where the report discusses the proposal by some states of "additional legally binding obligations", we advise that the text also reflect the views of a majority of states on the importance of ensuring the effective implementation of the existing framework of responsible state behaviour in the

[6] APC, Policy explainer "What is a gender-sensitive approach to cyber capacity building?", 2023, available at: https://www.apc.org/en/node/38840/.
[7] United Nations General Assembly, Open-ended working group in developments in the field of information and telecommunications in the context of international security: Final Substantive Report", A/AC.290/2021/CRP.2, para 56.

use of ICTs prior to any discussion of additional binding obligations. **We also recommend that paragraph 49 is amended to reflect the views of many member states that any future mechanism should embed open, inclusive and transparent modalities for the participation and accreditation of non-governmental stakeholders.**

- Paragraph 50: We welcome the commitment that the PoA should have as the foundation of its work the agreed normative framework of responsible state behaviour in cyberspace. **We recommend that text be added to paragraph 50(c) to reflect that the future mechanism should also allow for discussion of the development of new norms, CBMs and capacity-building measures, where needed and where relevant.**
- Paragraph 51: **We recommend that an additional sub-paragraph is added to paragraph 51 to reflects the proposals of many states that the PoA should also integrate and build upon the existing work of states and non-governmental stakeholders to develop guidance to ensure effective implementation of the agreed framework.**
- Cybersecurity is a team effort where stakeholders collaborate with states and provide assistance in a variety of ways, and a future mechanism should therefore incentivise states to collaborate with stakeholders. **The text in sub-paragraph 51 (d) should expressly reflect that the PoA should provide an "open, inclusive and transparent, sustainable and flexible process, <u>which promotes the participation of non-governmental stakeholders…</u>".**

Endorsed by the following organisations and individuals (as of 24 July 2023):

- **Access Now**
- **Association for Progressive Communications (APC)**
- **Centre for Multilateral Affairs (CfMA)**
- **Derechos Digitales**
- **Fundación Karisma**
- **Global Partners Digital**
- **IFEX**
- **Jokkolabs Banjul**
- **JONCTION**
- **Kenya ICT Action Network (KICTANet)**
- **Media Rights Agenda**
- **Red en Defensa de los Derechos Digitales (R3D)**
- **Professor Emeritus Wolfgang Kleinwächter, University of Aarhus, former ICANN Board Member**