INSTITUTO IGARAPÉ
a think and do tank

Igarapé Institute

Statement on the dedicated stakeholder session of the Open-Ended Working Group on security of and in the use of information and communications technologies.

27 July 2022

[First set of questions]

Dear Distinguished chair, delegates, and colleagues from other non-governmental entities,

We thank the chair and the member states for the opportunity to be here.

I am speaking on behalf of Igarapé Institute. We are an independent think and do tank dedicated to the areas of public, climate and digital security and its consequences for democracy.

As an organization that is based in Brazil and works primarily with countries in Latin America and global south, we see that stakeholders can play an even more important role in filling capacity building gaps and informing governments in their efforts to implement norms. And I highlight three ways:

- **First, stakeholders can help with Incident mapping and reporting** - from a developed but mostly developing country context, governments might face challenges in collating information about incidents. Sometimes relying on outsourcing their security and not necessarily developing internal capacities. We believe that CSOs (in joint efforts with other stakeholders) can help map incidents providing more situational awareness of national and regional contexts through open-source information. We recall the work of our colleagues from the Cyber Peace Institute on their efforts to track incidents against the healthcare sector. We have also been conducting incident mapping on ransomware and attacks against electoral infrastructure in Brazil in collaboration with other sectors to inform government entities and help develop preventive strategies based on that. **This is relevant to the implementation of norm 13(b) of the GGE report that calls states to consider all relevant information in the case of ICT incidents** – as it could, for example, support public attribution efforts.

- **Second, stakeholders can help identify gaps in cross-government efforts through national mapping of cybersecurity governance** - Governments sometimes are not aware of their counterparts or the norms that each respective department has already developed. That is why we launched the first nationally dedicated cybersecurity portal in Latin America – this case, focusing in Brazil. The Brazilian Cybersecurity Portal[1] provides a map of governmental and non-governmental actors nationally and collates all their normative efforts

[1] https://ciberseguranca.igarape.org.br/en/

(laws, decrees, whitepapers, joint statements).[2] We believe that Portals democratize the access to the cybersecurity debate for both governmental and non-governmental entities and, in our case, also complements the efforts of our colleagues at the international level (UNIDIR CPP)[3] and regional level (OAS Cybersecurity Observatory[4]). **We believe such efforts could inform the process of filling in of national surveys on norms implementation and capacity development as well as identification of Points of Contact beyond intra-governmental settings.**

- **Finally, stakeholders can help to promote interagency and multistakeholder best practices exchange** – We have developed a multistakeholder agenda for digital security[5] in Brazil based on meetings with stakeholders, which has resulted on the establishment of a multistakeholder platform for dialogue at the national level. **We believe this is in line with the implementation of norm 13d on information exchange.**

Thank you chair and we look forward to continuing the dialogue.

[Second set of questions]

Dear Distinguished chair,

Given the important task of member states this week to discuss the report, I would like to use this opportunity itself not to just answer what we could do as stakeholders to implement norms but to already provide input to the report as future implementation efforts will be guided by it. We will submit our complete comments with detailed recommendations for the text to the Secretariat, however, I would like to take these minutes to highlight four points:

- **On the question of gender**: We welcome the reference to it, recall the Women in Peace and Security agenda and note that the efforts of the OEWG would benefit from including a reference to it, thus linking cybersecurity to a transversal discussion to which gender is an integral part of. The connection between WPS and cybersecurity has already been recognised in different reports – and I mention UN Women's recent publication titled "Action Brief: Women, Peace & (Cyber) Security in Asia and the Pacific"[6] as an example that highlights the need to strengthen:
    - Women's participation in policy development and decision-making processes relating to cybersecurity;
    - The prevention of online-facilitated violence and conflict risks;

[2] https://ciberseguranca.igarape.org.br/en/ecosystem/
[3] https://cyberpolicyportal.org
[4] https://observatoriociberseguridad.org
[5] https://ciberseguranca.igarape.org.br/en/risks-and-recommendations/
[6] https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific

- **On human rights**: We believe that human rights should not be restricted to the International Law section of the Zero draft report and therefore propose that a mention be added to the introduction: Reiterating the commitment of member states with human rights through a reference to the norm 13(d) from the GGE 2021 report and paragraphs 1,2 and 3 of the OEWG 2021 report as well as on potential threats section we believe a mention could be added to how the **escalatory cyber threats landscape (with the latest being ransomware)** affects **disproportionately human rights defenders, civil society organisations, universities and societies alike.**

- **Also on existing and potential threats**: It is evident that states agree on the importance of protecting CI. We believe that Section B, would benefit from the characterisation how incidents against CI meet the international peace and security threshold, that is, through their scope, scale and speed. The inclusion of ransomware, attacks against healthcare, for example, would fall under that characterisation.

- **On capacity building**, we would recall paragraph 57 of the 2021 OEWG report and recommend the inclusion of a reference to south-south, north-south and triangular cooperation. We believe this could inform and contribute to the consolidation of more detailed discussion around capacity building.

Thank you chair.