Igarapé Institute

Recommendations to the Zero Draft Annual Report of the Open-Ended Working Group on security of and in the use of information and communications technologies.

27 July 2022

Comments and recommendations for the Zero Draft Annual Progress Report

Below we provide recommendations according to the sections outlined in the version shared by the chair on 22 July letter.

- We call states to avoid that geopolitical disputes disproportionately affect the participation of stakeholders, hindering an inclusive, diverse, and open debate. In the spirit of previous OEWG and recalling the 2019 intercessional as a landmark moment for stakeholder participation.[1]

- **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"[2] 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;

  We also highlight the recommendations from UNIDIR's "System Update: Towards a Women, Peace and Cybersecurity Agenda"[3] and believe it can serve as a guidance for the inclusion of gender-sensitive language in the report:
    - Acknowledge that the design and use of ICTs can affect men, women and other marginalized groups differently, and that gender considerations need to be applied to recognize the impact of ICTs on international peace and security;
    - Urge States to continue their ongoing efforts to increase the meaningful participation of women in organizations and intergovernmental processes examining ICTs;
    - Recognize the important role of civil society in discussions and negotiations around ICTs in the context of international peace and security; and

[1] https://cybertechaccord.org/industry-perspective-rejected-cybersecurity-tech-accord-regrets-decision-by-states-to-reject-participation-in-un-open-ended-working-group-on-cybersecurity/
[2] https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific
[3] https://unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda

- Encourage States to integrate gender considerations into the development of national cybersecurity policies.[4]

- **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(e) 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.**

  GGE 2021
  Norm 13 (e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression (A/76/135).

  OEWG 2021
  1. Despite the radical transformations the world has experienced since the United Nations was founded 75 years ago, its purpose and timeless ideals retain foundational relevance. ***Alongside the reaffirmation of their faith in fundamental human rights****, and their commitment to promote the economic and social advancement of all peoples and to establish conditions for justice and respect of international law, States resolved to unite their strength to maintain international peace and security.1*
  2. Developments in information and communications technologies (ICTs) ***have implications for all three pillars of the United Nations' work: peace and security, human rights and sustainable development.*** *ICTs and global connectivity have been a catalyst for human progress and development, transforming societies and economies, and expanding opportunities for cooperation.*
  3. The imperative of building and maintaining international peace, security, cooperation and trust in the ICT environment has never been so clear. ***Negative trends in the digital domain could undermine international security and stability, place strains on economic growth and sustainable development, and hinder the full enjoyment of human rights and fundamental freedoms.*** *These trends include the growing use of ICTs for malicious purposes.*

- **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.** We provide suggestions below:

[4] https://unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda

- Include reference to attacks against electoral infrastructure and healthcare sector as part of the CI threats characterisation. This could be done by referencing the GGE 2021 report paragraph 45.

  GGE 2021
  45. The COVID-19 pandemic heightened awareness of the critical importance of protecting health care and medical infrastructure and facilities, including through the implementation of the norms addressing critical infrastructure (such as this norm and norms (g) and (h)). ***Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes.*** *Critical infrastructure may also refer to those infrastructures that provide services across several States such as* ***the technical infrastructure essential to the general availability or integrity of the Internet****. Such infrastructure can be critical to international trade, financial markets, global transport, communications,* ***health or humanitarian action.*** *Highlighting these infrastructures as examples by no means precludes States from designating other infrastructures as critical, nor does it condone malicious activity against categories of infrastructures that are not specified above.*

- Mention to Ransomware *as an illustration* of the severe *effects* of attacks against CI. The threat landscape is in constant change and singling out one specific threat can be topical but time-bounded. To ensure the sustainability of the text agreed by the OEWG, the threats highlighted in the section could be thus read as an illustration of the threat landscape under CI. To better characterise how ransomware meets the threshold of international security, we propose two possible wordings:
  - Ransomware characterised in scale, scope and speed. OR
  - Ransomware meeting international peace and security threshold due to effects on national critical infrastructure.

- **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.

Guidance on stakeholder participation in norms implementation

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.

We strongly believe that **norms implementation should be considered a 'two-way street'**, **whereby governments should reach out to stakeholders** (namely civil society organizations, academic entities, private sector actors and technical community experts and bodies) **and vice-versa**. We believe that this has the potential to 'activate' concrete and actionable processes that are inclusive, innovative and have a well-situated perspective of the threat landscape.

We highlight three ways in which stakeholders can support norms implementation:

- **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.

  > *Norm 13 (b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences. (A/76/135)*

- **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[5] provides a map of governmental and non-governmental actors nationally and collates all their normative efforts (laws, decrees, whitepapers, joint statements).[6] 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

[5] https://ciberseguranca.igarape.org.br/en/
[6] https://ciberseguranca.igarape.org.br/en/ecosystem/

(UNIDIR CPP)[7] and regional level (OAS Cybersecurity Observatory[8]). **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.** And we recall, on this matter, norm 13(a) paragraph 21 of the GGE 2021, paragraph 30 and 65 of the OEWG 2021 report and paragraph 8(d) of the Zero Draft Annual Progress Report (July 22).

> *Norms 13(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.*
> *21. The measures recommended by previous GGEs and the OEWG represent an initial framework for responsible State behaviour in the use of ICTs. As further guidance, and to facilitate such cooperation, the Group recommends that States put in place or strengthen existing mechanisms, structures and procedures at the national level such as relevant policy, legislation and corresponding review processes; mechanisms for crisis and incident management; whole-of-government cooperative and partnership arrangements; and cooperative and dialogue arrangements with the private sector, academia, civil society and the technical community. States are also encouraged to compile and streamline the information they present on the implementation of the norms, including by voluntarily surveying their national efforts and sharing their experiences (A/76/135).*

- **Finally, stakeholders can help to promote interagency and multistakeholder best practices exchange** – We have developed a multistakeholder agenda for digital security[9] 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 13(d) from the GGE 2021 report on information exchange:**

> *Norm 13 (d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.*

[7] https://cyberpolicyportal.org
[8] https://observatoriociberseguridad.org
[9] https://ciberseguranca.igarape.org.br/en/risks-and-recommendations/