Global Partners Digital

Statements to OEWG on ICTs, 3rd session

27 July, 2022

Guiding questions #1:

Thank you Chair.

When we speak of the cyber capacity building landscape and how stakeholders are currently contributing, we must consider the wide range of activity and initiatives that relate to cyber capacity building, which broadly fall under five themes: cybersecurity policy, cyber incident management and critical infrastructure protection; cybercrime; cybersecurity culture and skills and cybersecurity standards. There are numerous examples of how stakeholders contribute to each of these areas, whether through the provision of training, legal and other expertise, the sharing of knowledge and good practice, development of resources and toolkits etc. But as I do not have much time, I wanted to share examples of how at GPD we have supported capacity building in relation to cybersecurity policy, including at the national level. Considering that National cybersecurity strategies, for example, are a key instrument for the domestication and implementation of the 11 norms this is particularly relevant.

For example, GPD engaged in the process of developing the most recent and 2nd edition of the "Guide to Developing a National Cybersecurity Strategy", an effort spearheaded by the ITU's Cybersecurity Program but implemented by a multistakeholder group of over 20 partners including the Council of Europe, Commonwealth Secretariat, Oxford's Global Cyber Security Capacity Centre, (INTERPOL), Microsoft, UNIDIR, among others.

We also work directly with a range of stakeholders and governments to support inclusive cyber policy development. We have developed practical toolkits on inclusive cyber policy development, and others for the assessment of cybercrime strategies and cyber policy strategies from a human rights perspective. GPD is also a partner of the Global Forum on Cyber Expertise and GPD works within the GFCE clearing house function which provides a matching service - where we have provided our expertise on the development of inclusive and rights-respecting national cybersecurity policies.

Recently we participated in the African School of Internet Governance/ AfriSIG (which included GPD as a partner this year), which brought together a diverse group of individuals from governments, law enforcement and security agencies, civil society organisations, digital rights and media groups, and cybersecurity experts from the region to identify cyber capacity building priorities and needs in the Africa region, the role of non-state actors in addressing these needs and concrete proposals for addressing them. The final output document will soon be available. This consultation shows how non-state actors play an important role in convening stakeholders, including governments, providing platforms for discussion, dialogue and collaboratively identifying priority actions for cyber capacity building. This is important because whatever aspect of cybercapacity building is being discussed, whether it is policy, diplomacy, technical skills or incident response, the strengthening of ties between people is at the heart of strong cyber capacity. We therefore recommend that in the report, the relevant recommendation which refers to surveying capacity needs nationally - reference the need to engage all stakeholders in such efforts, in order to ensure evidence-based, effective, sustainable capacity building initiatives and efforts.

Guiding questions #2:

Thank you Chair. With regards to these questions, Global Partners Digital is pleased to be able to deliver this statement to the OEWG but we regret that many stakeholders who would have had many relevant inputs to share on these questions are unable to do so as a result of the use of the veto against their accreditation. We hope that this will not remain the case going forward and the OEWG will be able to benefit from the rich array of expertise that is available from stakeholders.

In terms of contributing to the proposals, we would like to recommend that in developing additional guidance or checklists on norms implementation, elaborating and building upon the conclusions and recommendations agreed to in previous OEWG and GGE reports, as well as consider developing common understandings on technical ICT terms, states do so in consultation with stakeholders. In this way, states can build awareness of the norms but also ensure practical guidance is developed that is informed by realities and needs on the ground, of those who have expertise on existing regulatory frameworks, those who respond to threats and cyber incidents, and those who understand how those incidents impact people, communities and society. GPD has worked with other experts for example to develop the a series of briefs that unpacks the agreed framework on responsible state behaviour from a human-centric perspective, including the 11 norms. When it comes to surveying implementation, we also believe that states should work together with stakeholders and leverage their expertise and understanding of the policy landscape in their country to identify existing modes of implementation and gaps.

As recently recommended in the output document of AfriSIG which I referred to earlier, states should convene Inclusive open consultations to gather relevant input from non-state actors throughout the remainder of the OEWG's mandate on all issues on its agenda, not only on capacity-building. Non-stakeholder input can also add value to discussions on issues such as the applicability of international law, confidence building measures (CBMs) and norm development and implementation.

Regarding international law: the draft report The OEWG could convene discussions on specific topics related to international law and Capacity-building efforts on international law could be strengthened and could include workshops and training courses. Civil society organisations can and should support these efforts, particularly as they can bring legal expertise including from a human rights perspective and can provide necessary evidence, data and other information relevant to understanding the applicability of international law to cyberspace.

We'll provide a more detailed response in writing. Thank you.