OEWG Contribution - IGF BPF on Cybersecurity *(3 December 2019)*

(C) Rules, laws and norms: Stakeholders' commitments to rules, norms and principles: Tech Accord, Charter of Trust, Global Transparency Initiative, Paris Call and beyond

- ***What are the commonalities between the different multi-stakeholder initiatives on cybersecurity, such as the Tech Accord, the Charter of Trust, the Global Transparency Initiative, the Paris Call and other initiatives, and the norms developed at the intergovernmental level?***
- ***What synergies should be encouraged between intergovernmental and multi-stakeholder initiatives to prevent us going on separate paths?***

The Best Practices Forum, or BPF, is an intersessional activity of the Internet Governance Forum that has collected multistakeholder best practices on cyber security policy since 2014.

In 2018, the BPF worked to identify spaces of norms development across the community. We learned there are a lot of efforts outside of the UNGGE and the GCSC. This year, we identified 19 cybersecurity agreements and collected best practices on how signatories put these words to work. This included the Paris Call for Trust and Security in Cyberspace and the UNGGE 2015 consensus report.

I'll highlight a few findings:

- First of all, while discussions about what content should, and should not, be tolerated online is an important national and international dialogue, it is meaningfully different than discussions of cybersecurity. Conflating them can limit progress on one or the other.

- Contributors to the BPF determined key positive outcomes of these agreements. For instance, the inclusion of all stakeholder groups in the creation of cybersecurity agreements reinforces the shared nature of the challenge and builds agreement around the responsibilities all have. We also found that by clarifying roles and responsibilities, agreements and norms create obligations for identifiable actors and trigger more active accountability.

- We also determined adverse effects. Cybersecurity agreements are at risk of becoming counterproductive when they fail to focus on outcomes but instead prescribe a course of action; and cybersecurity agreements sometimes undermine human rights, which, in turn may reduce cybersecurity. This can be a result of them focusing on the security of the state, rather than the security of people.

- We learned that the quality of agreements can be improved by defining key terminology early; by avoiding needless ambiguity through multi-stakeholder inclusion in reviewing language; and by making capacity building a crucial part of any agreement.

At the IGF in Berlin, we brought in six experts to deepen our discussion. We identified a few additional learnings:

1. In our context, norms are collective expectations for what we see as proper behavior for an identifiable group. When organizations need to hide their behavior, it is often a good indication a norm may exist and is being violated. We also identified there's a second approach to norms development: identifying a behavior we aspire to and widely support, and then investing to implement it as a norm.
2. Despite the growth in norms initiatives there are areas of convergence. A number of initiatives are mapping these areas and we can consider them as a starting point for cooperation.
3. We can learn from highly technical norms efforts, such as Mutually Agreed Norms for Routing Security (MANRS), supported by the Internet Society, that are easier to measure and apply those lessons to less tractable problems.
4. As the representative from the Igarapé Institute mentioned yesterday, during the IGF, there was a proposed approach to scrutinize norms implementation through case studies of past events. Through the lens of history, we can evaluate norm effectiveness.
5. Only a relatively small number of agreements have so far been developed within clear multi-stakeholder spaces.

   We discussed several opportunities for improvement:
   a. Build networks, such as Communities of Interest, as proposed by the Global Commission on the Stability of Cyberspace, where stakeholders can cooperate on implementation;
   b. More multi-stakeholder engagement in the design of norms - stakeholders are often invited near the end, which is too late to ensure they can be implemented.
   c. It's clear that Civil Society has taken a leading role in assessing adherence to norms, this can be a basis for other multi-stakeholder approaches.

We believe there are beginnings of consensus expectations that we can all build on - **but they require the creativity that only multi-stakeholder and multi-disciplinary collaboration can bring to the table.**

More detailed learnings are available from our reports, published under the "BPF on Cybersecurity" section of the IGF web site (https://www.intgovforum.org/multilingual/content/bpf-cybersecurity).
Feel free to contact me should you want me to send you a copy.

Thank you very much.