**Key Takeaways from the Trust, Security & Stability Preparatory session IIGF2021**

**3 November, 2021**

While there is a need for collaboration the issue is how that can be done and the challenges around that. It is important to build on existing efforts among different communities and link them up together. The issue of resources first and political will versus need was highlighted along with the centralization of the networks and their impact on security and cyber security.

The issues related to specificity of definitions related to Cyber norms persist.There is a need to align understanding of what cyber norms include and that all refer to the same group of 11 non-binding norms agreed by States in 2015. To make norms work, it needs continuous discussion and effort for deepening the understanding of the multistakeholder community about how cyber norms work, what leads to success and failure in the norm implementation as well as engaging new actors. The discussion at the IGF should now focus on the implementation of those norms. Data governance need to be discussed within Cyber norms

Concerns were expressed over challenges in data flow owing to national regulations and the need to involve different stakeholders in discussions related to data governance issues. The issue on how to find a common consensus of data security and Internet governance was raised.

Cybercrime discussions require technical and policy solutions supported across the multistakeholder community. Governments need to take greater responsibility for criminal activity originating within their borders, even if the ultimate victims are elsewhere. However, combating cybercrime should not include stifling political speech or dissent, or other forms of free expression online. Any new cybercrime treaty should focus on ensuring effective exchange of information, reforming mutual legal assistance processes and finding ways to go after cybercriminals and not seek to undermine rights or seek to redefine or address things that are already addressed in existing agreements.
In terms of best practice, the Multistakeholder Manifesto on Cybercrime released by the Cybersecurity Tech Accord and the CyberPeace Institute was cited. It was observed that there are no sessions discussing the cybercrime treaty negotiations underway.

From the African and many developing country perspectives, several issues need to be addressed despite treaties on Cybercrime or conventions (that are not ratified by these nations). These include the cost for combating crime: the tools required, capacity building and necessary laws for its enforcement.

A need to formulate a better approach to dealing with existing cybersecurity challenges was highlighted. While it is universally accepted that cybersecurity cooperation and capacity building is crucial, a review of what has worked and what has not is necessary.

Affordability of security, lack of security budgets, lack of resources and capability of small businesses and governments, increasing threats of nation state actors when dealing with the cyber security incident and the issue of attribution were highlighted.

The example of CERTs and security researchers who volunteer to work together was highlighted as an example of cybersecurity cooperation. This cooperation extends not only to information sharing but capacity building too. Such initiatives need to be expanded, with continued support from other stakeholders.

The challenges related to capacity building include, lack of willingness to allocate resources for capacity building, poor participation, no followup post the capacity building exercise or lack of opportunities to actually practice what was taught. These need to be addressed at the higher level. Capacity building should not be limited to training but extended to mentoring, sharing information, inviting people to join the Community, collaborating to address issues and identifying and linking existing efforts to one another, e.g linking of table-top exercises run by corporates or states to work being done by CERT networks like FIRST.

On the issue of encryption, the need to get into the specificity of high level issues, such as who are you implicating, how is strong encryption defined, like were highlighted.
Stakeholders trying to own implementations and come up with alternative solutions that range from mitigation to training to actual implementations of some of these standards into their own products is needed. While most narratives related to the encryption discussion are focussed around  big tech companies, there are medium sized tech companies that are deeply affected by these issues.