Questions:

What are the typical roles and responsibilities of your/each of the stakeholder groups in making the internet a secure and safe place for people to socialize and conduct business?

As per global standard internet has been listed as one of the basic human rights. If we follow the norms most of the countries have signed to follow the international human rights charter where time and again policies and law keeps on changing as per need. As of today specially in developing nation the government has been in control and with the lack of proper resource and capacity they refuse to accept the local intervention of international norms and standards. They refuse to follow any sort communication channel in addressing the public voices in most of the cases "multistakeholder" representation is made which is highly discriminatory in terms of selecting individuals from choices and preference. The limitation of the approach result in lack of visibility where true voices and need of the time is sidelined. I think in terms of stakeholder groups' transparency in means of communication and visibility of information collection method is the most important thing that matters.

One thing we all have to understand is cyber security or policy should not be created for the sake of policy or law, it should be practical simple and should be able to cover each and every individual or else it's a discriminatory law or policy.

Typical roles of each stakeholder

-Proper collection of data and information
-Proper analysis of Information and communication
-Identifying problems and errors
-Proper dissemination of information
-Cooperation and developing means of Trust

What are some of the typical communication mechanisms between stakeholder groups to discuss cyber security related concerns?

The typical communication mechanisms between stakeholder groups to discuss cyber security related concern are

-National Internet Governance Forum
-Workshops and conference on cyber security
-Discussion of Research and Report communication of data and information
-Analysis of cyber security situation
-National Crisis situation

How can cybersecurity cooperation and collaboration be enhanced particularly in developing and least developed countries?

Cyber security cooperation and collaboration is an important aspect of knowledge sharing and communication process which needs greater efficacy in terms of its knowledge and management. In most of the case of the developing and least developed countries even at leadership and policy making level people will have no idea about cyber security and internet governance process. The limitation of ideologies and lack of communication in-terms of technology update is something that seriously hinders the overall internet governance process. I think at first capacity and awareness program about the internet governance process is a must and after that regional and national internet governance forums can play a tremendous role in terms of cybersecurity cooperation and collaboration in developing and least developed countries

What are some common problem areas that stakeholders encounter when trying to enhance cooperation and collaboration?

The problem areas that stakeholders encounter when trying to enhance cooperation and collaboration
- Government trying to act as a regulator not facilitators
-Orthodox and limited mentality (Political leadership)
-Limitation of laws and policies
-Lack of cooperation from the government
-Lack of standardization
-Lack of acceptance of open standards
-Lack of proper core values of internet
-Lack of platform (National IGF)
-Lack of resources and infrastructure
-Quality of standards
-No proper communication channel

What are some notable existing best practices and examples of successful collaboration and cooperation amongst stakeholders and specific actors that have helped improve cybersecurity?

I think in most of the cases looking at the current practice, until and unless the government decided to come front with its role of facilities things are always hard in terms of cooperation and collaboration. The best notable existing best practices and examples of successful collaboration and cooperation amongst stakeholders and specific actors that have helped improve cybersecurity is National Internet Governance Forum which helps to provide proper indication of various factors of the industry.

Contribution to IGF 2016 Best Practice Forum Cybersecurity by Shreedeep Rayamajhi Rayznews

What are some examples of best practices in 'Cyber security Situational Awareness' where different organizations have worked together, specifically with law enforcement agencies and other specialists?

As compared to developed nations, the limitation of cyber security situational awareness is something that is clearly lacking in developing and least developed countries. If you look at the current practice the limitation of cyber security is just limited within the policies and law which are virtually meaningless in terms of the technology and adaptation. Moreover, there is a situation of complexity where in most of the developing countries you will see either there is no knowledge of it or if there is a knowledge also there is complexity of understanding which enforces many Cert teams and cooperating agencies and mechanism in terms of action and communication.

What are other related or different topics that your organization would like this BPF to address moving forward, both in 2016 and beyond?

I think most important topic in terms of Cyber security are listed as below

1. Awareness and capacity building in terms of cyber security
2. Common problems of policy mechanism and action
3. Lack of policy upgrading and communication
4. Cooperation and collaboration in between agencies at national and regional level
5. Complexity of multiple cyber security agencies and their management
6. Integration & adaption of open standards in terms of cyber policy and mechanism