



## BPF on Cybersecurity 2017 - Call for Contributions

➤ **How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?**

Cyber security is not just the sense of being safe, it's the overall confidence of being safe where people know what is right and wrong. They are more responsible to the system and they act upon. This helps them to further create and innovate better environment of creating better solutions. Sustainable Development Goals certainly support the role of capacity building, better awareness program and discussing about the developing core values at grassroots level. But one thing we have to understand is Multistakeholder is not just about diversity or participation, it is more about inclusion and reaching out to the marginalized and unreachable communities. So certainly its more like cybersecurity helps to build confidence and confidence helps to build the motivation and SDGs drives that energy towards achieving the goals.

➤ **How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?**

The poor cybersecurity hinders the growth and trust in ICTs and internet technology at various levels

- Policy Level
- Leadership Level
- Individual Level

At policy level with lack of proper cyber security proper policies would not be able to develop. There are many issues of sovereignty and security of a country which needs privacy and certain level of secrecy in terms of policy level. These decisions of leadership not only decide the future of the country but are strategic assumption of its position which needs top level security and precision.

At leadership level if there is no cyber security the countries position can be compromised with no option of process.

At individual level if there is no leadership and policy there is no direction and people follow leaders

So lack of proper cyber security certainly effects the ability to support SDGs and its implementation

➤ **Assessment of the CENB Phase II policy recommendations identified a few clear threats. Do you see particular policy options to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:**

- Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services
- Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments
- Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended
- Confidentiality and availability of sensitive information, in particular in medical and health



## BPF on Cybersecurity 2017 - Call for Contributions

services

- Online abuse and gender-based violence
- Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Point (IXP) communities
- Vulnerabilities in the technologies supporting industrial control systems
- Use of information collected for a particular purpose, being repurposed for other, inappropriate purposes. For instance, theft of information from smart meters, smart grids and Internet of Things devices for competitive reasons, or the de-anonymization of improperly anonymized citizen data
- The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis
- Unauthorized access to devices that take an increasing role in people's daily lives
- Other: describe a cybersecurity issue critical to developing the SDGs in ways not listed above relevant to your stakeholder community (100 words or less)

### -Social media and its interventions and interpretation

I think more or less the above issues are correlated with the internet of today's but with the evolution of social media and cyber terrorism adapting and creating vacuum to reach out, there seems to be a great threat in terms of how the social media is transforming in today's world. For instance

**Cyber Terrorism-** The extremist group are targeting the vulnerable community and reach out using various platform to disseminate and create a larger network of access

**Online safety-** There are various social media platform which are evolving that are targeted or being wrongly used for cyber bullying, pornography and as a tool of online harassment. These things may look small but when looked at from the gender and other lens the crack they are creating are very vast and unrepairable

We have work on a greater heightened awareness and capacity building program that can empower people to look beyond the problem and act accordingly.

- **Many Internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community or private sector, and used by other communities and interact in unexpected ways. Stakeholders are managing complexity. This both shows the strength and opportunities of ICTs and Internet Technologies, but also the potential risks. New technologies may be insufficiently secure, resulting in harms when they are deployed: conversely we may adopt security requirements or measures that prevent the development, deployment, or widespread use of technologies that would generate unforeseen benefits. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?**

Humans survived the 4.5 billion years evolution not because they are smart or they have the attitude. They survived because they could learn and by their nature of innovation and adaptation. We are progressive beings where we trial and test new technology using our effectiveness and efficiency to direct the collaboration. We learn and we destroy, the ideology of destruction is not just about ending but about creating better. I strongly believe it's in our nature of not being satisfied and that's what drives us. The current competition and aspect of being in control is the current problem but as I said



## BPF on Cybersecurity 2017 - Call for Contributions

destruction is not the end, it's a new beginning that is the reason why we are always looking at better ways of evolution. Potential risk are inevitable situation which cannot be escaped but can be further worked and collaborated in adaptation process.

Similarly, talking about Technology and multistakeholderism it's the main issues of how we will developed the core values. As the world believes in democracy and people's power where technology drives the system and core values drive the people and people are driven by leaders with better core values.

So the priority is to work on developing greater set of core values which will guild the system in creating better ways of securing internet and creating better values for cyber security.

The responsibilities lies at the basic level of how we accept standardization and adopt unified set of values in terms of equality, cooperation and collaboration for all

One world internet and one religion Humanity

The first issue in terms of developing nation is to develop better core values and creating better awareness programs for leadership in understanding multistakeholderism in the internet ecosystem

As an outside expert consultation or consolidation cannot help the adaptation process rather it will create loop hole. The adaptation need to be done at first stage of how internet is perceived or used creating broader picture of adapting global standards.

As the internet is changing day by day things need to be smart and precise. The whole process of adaptation and standardization needs to be in basic core values where there needs to be equality and concept of collaboration of creating better values.

- **What is for you the most critical cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF? Should any stakeholders be specifically invited in order for this issue to be addressed?**

I think for a country like Nepal we need to develop better core values and we need recognized as individual country where our issues are unique from any other country in the region. The current state of developed nation pushing developing and least developed countries has created a gap which caters externalities. For example Asia in global IGF or platform is either lead by India or china or any other big country where as in reality these country have stronger policy mechanism, awareness level and adaptation process which needs no recognition. From MAG appointment to other IGF leading process members from least developed countries are marginalized in ways of geography, population and other interventions.

But at ground reality smaller and least developed countries suffer the burden and consequences of being limited within their limitation. The standardization and adaptation process creates smaller ways of intervention where it is limited by resisting attitude in driving the industry. Technology has just been passed on to the developing or least developing countries just for the sake where from our side we played our part of making it the technology of today but when it comes to representation and opportunities. We are marginalized in various ways.

**We need representation and opportunity at global IG process.**

Though least developed countries name has been highlighted in the IGF mandate but if you check it from participation, representation we have been.



## **BPF on Cybersecurity 2017 - Call for Contributions**

Shreedeeep Rayamajhi