2017 IGF Best Practice Forum on Cybersecurity

Dear National and Regional IGF representatives,

The IGF Best Practices Forum on Cybersecurity is calling for input for its 2017 effort. We are very interested in understanding national and regional specifics on the cybersecurity challenges we all face, and are looking for your assistance.

During 2015 and 2016, the Policy Options for Connecting and Enabling the Next Billion(s) (CENB) activity within the Internet Governance Forum identified two major elements:

- Which policy options are effective at creating an enabling environment, including deploying infrastructure, increasing usability, enabling users and ensuring affordability;
- How Connecting and Enabling the Next Billion(s) contributes to reaching the new Sustainable Development Goals (SDGs).

The Best Practice Forum on Cybersecurity realizes that making Internet access more universal, and thus it supporting the SDGs, has significant cybersecurity implications. Well-developed cybersecurity helps contribute to meeting the SDGs. Poor cybersecurity can reduce the effectiveness of these technologies, and thus limit our opportunities to helping achieve the SDGs. In our 2017 effort, we aim to identify policy mitigations that can help ensure the next billion(s) of users can be connected in a safe and reliable manner.

BPF members have already performed some security focused analysis of the CENB Phase I and II documents developed during previous years. You can review these documents here:

Security focused reading of CENB Phase I - https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/687
Security focused analysis of CENB Phase II - https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/688

You can assist in the BPF by sending us answers to any or all of the following questions. They are divided in two sets:

- *General questions* should be relatively easy to answer, and provide a strong contribution to the BPF. Thank you in advance for addressing these.
- *Specific questions* are focused on very specific areas of interest. We do not expect you to respond to all of them, but if you have the opportunity to discuss them in your NRI, we welcome your input.

You are invited to share your responses on the BPF mailing list (*https://www.intgovforum.org/mailman/listinfo/bp_cybersec_2016_intgovforum.org*). For any questions, you can reach out to the Secretaria at igf@unog.ch with in cc lead expert Mr. Maarten van Horenbeeck (maarten@first.org), and the BPF's co-facilitators, Mr. Olusegun Olugbile (solugbile@gmail.com) and Mr. Markus Kummer (kummer.markus@gmail.com).

Thank you,

Markus Kummer
Olusegun Olugbile
IGF BPF on Cybersecurity co-facilitators

Questionnaire

Full Name of the NRI you are responding for:

Your name and official role at the NRI you are responding for:

- ❑ Coordinator
- ❑ Chair or co chair
- ❑ Member of the Steering Group/Organizing Committee/MAG of the NRI [describe which]
- ❑ Interested participant/observer in an NRI
- ❑ An NRI community member
- ❑ Observer on the NRIs mailing list

Your contact information (e-mail):

General questions

- Has your NRI organized a session on cybersecurity? Was it considered a priority session?
- For how many years has your NRI covered cybersecurity as a topic?
- What did the session address, or was covered in the session agenda? Were any implementation plans or policy proposals presented or discussed at your meetings, or discussed during intersessional work?
- What were the main outcomes, or work initiated out of this session?
- Does your NRI maintain any key messages on cybersecurity?

Specific questions

- What working definition do you maintain for cybersecurity? What is considered a cybersecurity issue and what is not?
- 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)?
- 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)?
- Assessment of the CENB Phase II policy recommendations identified a few clear threats. Which of the following do you consider priorities? Do you see particular policy options or best practices to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:
    - Issues that impact the reliability and access to Internet services
      Priority? Yes/No
      Policy options?
        -

-

- Security of mobile devices
  Priority? Yes/No
  Policy options?
  -
  -

- Potential abuse by authorities, including surveillance
  Priority? Yes/No
  Policy options?
  -
  -

- Confidentiality and availability of sensitive information
  Priority? Yes/No
  Policy options?
  -
  -

- Online abuse and gender based violence
  Priority? Yes/No
  Policy options?
  -
  -

- Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Points (IXP)
  Priority? Yes/No
  Policy options?
  -
  -

- Vulnerabilities in the technologies supporting critical industrial processes such as electricity provisioning
  Priority? Yes/No
  Policy options?

        -
        -

    - De-anonymization of improperly anonymized citizen data
      Priority? Yes/No
      Policy options?
        -
        -

    - The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis
      Priority? Yes/No
      Policy options?
        -
        -

    - Internet of Things security.
      Priority? Yes/No
      Policy options?
        -
        -

    - Human Factors and security awareness and education
      Priority? Yes/No
      Policy options?
        -
        -

    - **Other**: describe a cybersecurity issue critical to developing the SDGs in relevant to your nation or region (100 words or less)
      Priority? Yes/No
      Policy options?
        -
        -

- Please, enumerate Innovative Practices in the field of cybersecurity that you have seen discussed in your community, and which help promote the safe connection of the next billion(s) of users, or promote the Sustainable Development Goals.

- 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?

- Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

- 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?