2017 IGF Best Practice Forum (BPF): Cybersecurity – Virtual Meeting III

Summary Report

7 August 2017

1. The IGF Best Practice Forum (BPF) on Cybersecurity held its third virtual meeting on 7 August 2017. The meeting was facilitated by Markus Kummer. The primary purpose of the call was to review the different elements of the BPF's call for contributions, namely, the list of contacts to reach out to, the message to contributors, and the questionnaire. A recording of the meeting is available here: https://intgovforum.webex.com/intgovforum/ldr.php?RCID=4715eb63b363868608f25acd5c63c1d7

2. The meeting began with an overview of the list of contacts compiled by the members of the group. The list, shared among BPF members in an editable document, contains more than one hundred names of individuals and organizations with relevant cybersecurity expertise, from all stakeholder groups, including Governments. Only a small number of contact addresses were missing at the time of the call, and several members volunteered to help fill these gaps, especially where Government contacts are concerned and within stakeholder groups they are strongly connected to. One member, Richard Leaning, offered to assist in communicating with regional Internet registries (RIRs) specifically. The Secretariat could also help fill remaining gaps. All were invited to submit any contact details for the list to BPF lead expert Maarten van Horenbeeck or to the Secretariat directly.

3. Maarten then briefed participants on the message to contributors and draft questionnaire, shared on the mailing list before the meeting (**ANNEX II**). The questionnaire incorporates the analyses of the Connecting and Enabling the Next Billion(s) (CENB) Phase I and II documents previously drafted by Maarten and Andrew Cormack, respectively (available here and here). Drawing primarily from the CENB II analysis, which looked at how policies for enabling connectivity and supporting the Sustainable Development Goals (SDGs) could have cybersecurity implications, the questionnaire seeks public input on any additional cybersecurity risks identified in this context and recommendations on how to mitigate them. Beyond its focus on the SDGs, the questionnaire also asks respondents to weigh in on the responsibilities of different stakeholders for mitigating risks, as technologies emerge in uncoordinated ways and generate challenges unpredictably. It includes,

finally, a question proposed by BPF member Wout De Natris, on which cybersecurity issue respondents feel is most critical today.

4. BPF members responded very positively to this draft, which was seen as clear, concise and sufficiently high-level so as to include a wide spectrum of institutional and individual views. To further ensure the questionnaire generates the desired quality of responses, Alejandro Pisanty volunteered to translate the questionnaire into Spanish.

5. There was a general understanding that National and Regional Initiatives (NRIs) would be important contributors to the process. In particular, they would be well placed to seek input from their respective Governments. Marilyn Cade suggested drafting a two-page introduction to the BPF process for NRIs, which Maarten offered to do with inputs from others. It was also suggested NRIs be given a short briefing on the questionnaire in one of their calls.

6. Other comments on the questionnaire related to the specific wording of some questions, as well as on the possibility of adding an "other" option in which a respondent could make a contribution in a free-form way. Markus suggested adding the BPF's meeting summaries to the "Relevant Reading" list, in order to give respondents an idea of the process leading to the questionnaire. Alejandro cited the longstanding issue of contrasting multistakeholder and multilateral approaches to cybersecurity, and the need to properly transmit the questionnaire to officials in Governments. The draft questionnaire will in any case remain open for comments and suggested edits until it is sent out for inputs on or around 15 August.

7. The following next steps were established by the BPF:

   -Members are to make any **final comments or suggest edits** on the questionnaire and call for contributions **before 15 August**.

   -Any remaining **contact details for the contributors list** should be sent to Maarten and/or the Secretariat **before 15 August**.

   -The Secretariat will **send out the call and questionnaire** on or around **15 August**.

   -The **deadline for contributions** is **15 September**, although the BPF can exercise flexibility in accepting contributions past this date. The Secretariat will publish contributions as it receives them.

8. BPF members agreed their next meeting should take place shortly after the 15 September deadline, in order to review the full list of contributions.

Annex I – Participants List

Markus Kummer (Facilitator)

Eleonora Mazzucchi (IGF Secretariat)

Oscar Avila

Carina Birarda

Marilyn Cade

Andrew Cormack

Jose de la Cruz

Lucimara Desidera

Zama Dlamini

Maarten van Horenbeeck

Laxmi Khatiwada

Richard Leaning

Ithabeleng Moreke

Alejandro Pisanty

Juan P. Salazar

Tomslin Samme-Nlar

Tom van Schie

Jesse Sowell

Timea Suto

Annex II – Draft Call for Contributions and Questionnaire

Call for contributions:

All stakeholders are invited to submit written contributions addressing the below questions and issues to the 2017 IGF BPF on Cyber security mailing list (subscribe: https://www.intgovforum.org/mailman/listinfo/bp_cybersec_2016_intgovforum.org) by 15 September 2017. While it is envisioned that initial drafting of the output document will begin on 15 September, this should be considered a soft deadline as contributions will be welcome after the 15th of September, particularly contributions from IGF National and Regional Initiatives (NRIs) and from other relevant entities or organisations who may be holding meetings relating to cybersecurity prior to the IGF annual meeting in December.

Contributions will then be compiled and synthesized by the Secretariat, and further circulated to the community for comment and further work towards an output document for the BPF to be presented at the 12th IGF in Geneva, Switzerland from 18-21 December.

All individuals and organizations are asked to kindly try to keep their contributions to no more than 2-3 pages, and are encouraged to include URLs/Links to relevant information/examples/best practices as applicable. When including specific examples or detailed proposals, those may be included as an Appendix to the document. Please attach contributions as Word Documents (or other applicable non-PDF text).

Overview:

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 Practices 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.

BPF participants have conducted an initial study of how the policy proposals compiled as part of CENB Phase I and II may affect, or be affected by, cyber security implications.

As part of this ongoing effort, the IGF is now calling for public input to collect additional risks and cyber security policy recommendations that can help mitigate security impacts, and help ensure ICTs and the Internet continue to help contribute to achieving the SDGs.

Relevant reading:

- UN Sustainable Development goals - http://www.un.org/sustainabledevelopment/sustainable-development-goals/
- Policy Options for Connecting & Enabling the Next Billion(s) - Phase II https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3416/549
- Security focused reading of CENB Phase I - https://www.intgovforum.org/[link to be completed]
- Security focused analysis of CENB Phase II - https://www.intgovforum.org/[link to be completed]

Questions:

- How does good cybersecurity contribute to the growth of ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?
- How does poor cybersecurity hinder the growth of 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. 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 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

- Many internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community, and used by other communities in unexpected ways. This both shows the strength and opportunities of ICTs and Internet Technologies, but also entails risks. Risks are rarely balanced ahead of time, resulting in incidents, and the network and its users adjust and make changes along the way. 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 cyber security 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?