# 2016 IGF Best Practice Forum (BPF): Cybersecurity – Virtual Meeting V

## Summary Report

## 19 September 2016

1. The fifth virtual meeting of the 2016 IGF Best Practice Forum (BPF) on cybersecurity was held on 19 September 2016. The meeting was facilitated by the IGF Secretariat. The primary purpose of the call was to review a draft outline/framework of the BPF output which had been circulated by the Secretariat prior to the call and had been made available for public comment in a google doc. This draft outline is included here as **ANNEX I**. It was reported that significant progress had been made in collecting inputs from the community for the output since the last virtual meeting on 16 August. The Secretariat noted that a first full draft version of the output would be made available in the coming weeks for further review and comment by the community, and that during this period (September-October) further contributions would also be welcomed and added to the output if applicable in an attempt to offer multiple points of entry into the work for the community, including contributions from National and Regional IGFs (NRIs).
2. It was also reported by the Secretariat that two additional virtual meetings would be convened prior to the 1 November initial deadline when the draft output would be posted publically using an online review platform for wider comments in the one month period leading up to the 11th IGF in Guadalajara, Mexico. In addition to using these meetings to allow further review and comment on the draft output, the meetings will also be used to plan the substantive session of the BPF at the IGF annual meeting from 6-9 December. This will be a 90 minute session, though the date and time for the session has not yet been confirmed.
3. A number of useful comments and suggestions were made during the open discussion on the ongoing work of the BPF and on the first version of the draft outline. A representative from the Freedom Online Coalition reported that an IGF Day O event was being planned in partnership with the BPF on the topic of enhanced cooperation and communication between actors working on cybersecurity. Stakeholders involved in the BPF will of course be invited to join this session and future virtual meetings of the BPF may be used to help shape this event.
4. Some stakeholders noted the importance of engagement with the law enforcement communities, particularly in developing countries, and suggested that Best Practice collection and dissemination would most benefit these groups. It was also suggested that the output could further define the term cybersecurity as it was said by some to

be too broad and that further refining the term and what the BPF means when it refers to cybersecurity would be important. It was also suggested that the BPF work leading up to the meeting and perhaps also in 2017 could extend the notion of identifying best practices to help identify actual cybersecurity decision-making practices. One stakeholder also suggested that the work could also explore more the topic of open standards and open data as they relate to cybersecurity efforts.

---

## Annex I

***Draft Overview/Outline as of 19 September 2016***

### 2016 Internet Governance Forum (IGF) Best Practice Forum (BPF) on Cybersecurity:

**'Building Confidence and Security in the use of Information and Communications Technologies (ICTs) through Enhanced Cooperation and Collaboration'**

### Part I: Framing the 2016 IGF BPF Cybersecurity Multistakeholder Dialogue

**A) IGF 2015 Main Session On Enhancing Cybersecurity and Building Digital Trust (12 November 2015) :** http://www.intgovforum.org/cms/documents/igf-meeting/igf-2015-joao-pessoa/igf2015-reports/609-igf2015enhancing-cybersecurity-and-building-digital-trust

*"The general consensus coming from the session was that cybersecurity is everyone's problem and everyone should be aware and understand that the cyber world is a potential unsafe place. A culture of cybersecurity is needed on different levels. Individual action was encouraged to make the Internet safer. Moreover, a need for a comprehensive approach to tackling cybercrime and building trust, such as the introduction of security elements when developing cyber products and services, was highlighted. Participants also stressed the critical role that education plays in addressing cybercrime issues and noted that education should be expanded to involve all levels of society. Capacity-building was cited as an indispensable driver for cybersecurity.*

*There were calls for further multistakeholder participation in the tackling of cybercrime. Session panellists agreed that the IGF, including national and regional IGFs, has proven to be a good collaborative multistakeholder process for cybersecurity, but still needs to reach out to get missing parties around the table. The involvement of the government, private sector, civil society and other stakeholders in handling cyber security was stressed as fundamental in terms of sharing best practices, sharing results of critical assessments and identifying globally accepted standards of cybersecurity. All stakeholders must understand, respect and trust each other's expertise and competences."*

**B) During the IGF MAG meeting from 4-6 April, there was agreement that a 2016 BPF would be carried out on a cybersecurity related topic/theme, building upon the previous work of the CSIRTS and SPAM BPFs.** The MAG meeting also acknowledged that the WSIS +10 review process has produced an outcome document with a strong focus on "building confidence and security in the use of information and communications technologies", making an IGF BPF related to cybersecurity even more relevant.

**C) While reviewing the outcomes of both the IGF Spam and CSIRT Best Practices Forums (BPFs) held in 2014 and 2015, there was an emerging consensus amongst the community that the 2016 cybersecurity BPF would benefit from addressing cooperation and collaboration between stakeholder groups as a topic.** The community also expressed that all stakeholders would benefit from having a multistakeholder discussion, including each of the major IGF stakeholder groups, on how to engage and communicate with each other on cybersecurity issues. There was also a feeling that this would be uniquely fit for an IGF BPF. There was also an emerging agreement that the BPF for 2016 should not be seen in isolation, but should rather be seen in a long-term perspective and that capacity building would be an integral component for the work. End users, law enforcement agencies, policymakers, and all of the other range of actors involved in cyber security, can be reached out to and involved in the work. National and Regional IGF initiatives (NRIs)s could also play an important role in feeding their discussions into the work, and vice versa.

**D) Initial Contributions/Ideas/Suggestions received via emails on BPF Cybersecurity Mailing List:**
Proposal from: Andrew Cormack, *Jisc*Adli Wahid, *FIRST*, Cristine Hoepers, *CERT.br/NIC.br* Peter Cassidy, *Anti-Phishing Working Group (APWG)*, Maarten Van Horenbeeck, *FIRST*, Serge Droz, *FIRST*; Neil Schwartzman; Jerome Athias; James Gannon; Serge Droz; Marilyn Cade; David Strudwick; Michael Ilishebo; Alejandro Pisanty; Wout DeNatris; Cheryl Miller; Nick Shorey; Richard Leaning and more.

**E) Contribution from Mr. David Strudwick, Positioning Brief - Cybersecurity Situational Awareness**

**F) Contributions from the Internet Society (ISOC):** ***A policy framework for an open and trusted Internet* – http://www.internetsociety.org/doc/policy-framework-open-and-trusted-internet *and Collaborative security approach to tackling Internet security* issues: http://www.internetsociety.org/collaborativesecurity**

**G) Asia-Pacific Regional IGF (27-29 July 2016) Synthesis Document :** http://comment.rigf.asia

**H) 2016 European Dialogue on Internet Governance (EuroDIG) (9-10 June 2016):**

- Transcript: Cybersecurity revisited, or are best practices really best?
- Transcript: From cybersecurity to terrorism - are we all under surveillance?
- Transcript: The future of cybersecurity in Europe - from state of play to state of art

**I) www.againstcybercrime.org**

## Part II: Synthesis of contributions received in response to the call for contributions

**Contributions:**

- **Contribution from Mr. David Strudwick, Positioning Brief - Cybersecurity Situational Awareness**
- **Contribution from the Freedom Online Coalition Working Group 1 - "An Internet Free and Secure"**
- **Contribution from Mr. Fojon Kosta, Government of Albania Contribution from Mr. Fojon Kosta, Government of Albania**
- **Contribution from Mr. Olusegun H. Olugbile, Member National (Nigeria) Advisory Council on Cybercrime**
- **Contribution from the DiploFoundation: *Cybersecurity Competence Building Trends -* http://www.diplomacy.edu/ig/cybersecurity (*the links to the full report and the illustrated executive summary, versions for download and for review*)**
- **Contribution from the Nigeria IGF (NIGF)**
- **Contribution from Mr. Jerome Athias: https://www.helpnetsecurity.com/2016/07/13/security-vendor-collaboration/**
- **Contribution from Mr. Shreedeep Rayamajhi, Razynews**
- **Internet Governance Capacity Survey: Nepal (Submitted by Mr. Shreedeep Rayamajhi)**
- **Contribution from the Internet Society (ISOC): *A policy framework for an open and trusted Internet* – http://www.internetsociety.org/doc/policy-framework-open-and-trusted-internet**
- **Contribution from the Internet Society (ISOC): *Collaborative security approach to tackling Internet security* issues – http://www.internetsociety.org/collaborativesecurity**

- **Contribution from the Association for Progressive Communications (APC)**
- **Contribution from The Information Technology - Information Sharing and Analysis Center (IT-ISAC)**
- **Contribution from the Organization of American States (OAS)**
- **Contribution from the Forum of Incident Response and Security Teams (FIRST)**
- **Contribution from Global Partners Digital**
- **Contribution from the National Cyber Security Centre - Finland (NCSC-FI)**
- UNODC Cybercrime Repository

**Questions/Synthesis Structure:**

- 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?
- What are some of the typical communication mechanisms between stakeholder groups to discuss cyber security related concerns?
- How can cybersecurity cooperation and collaboration be enhanced particularly in developing and least developed countries?
- What are some common problem areas that stakeholders encounter when trying to enhance cooperation and collaboration?
- What are some notable existing best practices and examples of successful collaboration and cooperation amongst stakeholders and specific actors that have helped improve cybersecurity?
- 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?
- What are other related or different topics that your organization would like this BPF to address moving forward, both in 2016 and beyond?

## Part III: Summary of 2016 BPF Dialogue/Contributions *(including discussions in the leadup to IGF 2016 and during dedicated substantive BPF session at IGF 2016)* and recommendations for way forward

**A. Comments received from community on Draft 1.0 of output document**

**B. Comments received + summary of discussion at IGF 2016 dedicated BPF session (6-9 December 2016)**

**C. Recommendations for way forward for BPF and messages from BPF to feed into other relevant fora/processes**