**BPF Cybersecurity 2019 – note of meeting 1**

- Meeting 1a: 12 March, 15:00 UTC. Recording of the meeting can be found here
- Meeting 1b: 20 March, 06:00 UTC. Recording of the meeting can be found here

The first meeting was about scoping the work for 2019. It comprised of two calls, with the aim of covering the same material on both calls and for people to only need to call in to one meeting.

**Item 1) Walkthrough of the approved BPF proposal for 2019**

This was a short item to provide context for the rest of the meeting, reviewing the description of the planned work of the BPF Cybersecurity in 2019 on "Exploring best practices in relation to recent international cybersecurity initiatives". The proposal was approved by the IGF Multistakeholder Advisory Group (MAG) on 12 February, circulated to the BPF on 13 February and can be found here - http://www.intgovforum.org/multilingual/filedepot_download/4904/1531.

**Item 2) Agreements to cover**

This item was about the agreements and processes that should be cover by the BPF in its 2019 report. The idea is to look for agreements or initiatives with multiple signatories from different stakeholder groups, and to seek to identify a number of elements which appear in two or more agreements. These horizontal elements would become the focus for the 2019 BPF on Cybersecurity.

The BPF Lead Expert, Maarten van Horenbeeck, shared written suggestions on the BPF mailing list ahead of the meeting in preparation for the discussion of this agenda item:

> *I wanted to share some of the agreements and processes that we distilled either in this year's proposal, or in the work last year, which we may consider for our BPF:*
> - *Paris Call: launched by France at the IGF, currently has 547 official supporters, including 65 states.*
> - *UNGGE: Its 2015 consensus report proposed several norms, rules and principles for the responsible behavior of States. A new group being established in 2019 will continue to explore this topic.*
> - *OEWG: This new 2019 group will reportedly study the norms proposed by prior UNGGE and identify potential new ones.*
> - *Tech Accord: A set of commitments promoting a safer online world through collaboration among technology companies.*
> - *Charter of Trust: A set of companies endorsing minimum general standards for cybersecurity through ten principles.*
> - *GCSC Six Critical Norms: A set of six new norms proposed by a multi-stakeholder group intended to improve international security and stability in cyberspace.*
> - *Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security: The FOC's Working Group 1 frames cyber security approaches in a human rights context.*
> - *SCO's Agreement on cooperation in the field of ensuring the international information security: Member states of the Shanghai Cooperation Organization agree on major threats to, and major areas of cooperation in cybersecurity.*
>
> *With the exception of the 2019-2020/2021 work of the UNGGE and OEWG, these all have in common that they contain a set of shared agreements or commitments on how to address cybersecurity issues through*

*mutual cooperation. Each of these also looks at the issue from the perspective of a different stakeholder community.*

During the discussion, it was noted that the UNGGE and OEWG would not complete any outputs in 2019, but that several MAG members had expressed a desire for these UN initiatives to be taken into account in the BPF's 2019 work. It was agreed that the BPF should seek to feed its report into those processes, e.g. ahead of the first GGE session (5-13 December, 2019) and ahead of the second substantive OEWG session (10-14 February, 2020). An indicative timeline for the UN initiatives can be found here.

It was also noted that the Global Commission on the Stability of Cyberspace (GCSC)'s six new norms are going through a review process. It was agreed that it would be sensible to focus on the norms which are more stable and the BPF Lead Expert will contact the GCSC secretariat to understand the timeline for finalizing the norms, and their respective stability.

Other agreements / initiatives that were suggested included:

- African Union Convention on Cyber Security and Personal Data Protection
- Council to Secure the Digital Economy International Anti-Botnet guide
- UN High-Level Panel on Digital Cooperation – this is not purely focused on cybersecurity and it might be too high-level compared to the other cybersecurity-specific agreements under consideration, but it was agreed that the BPF should look at the HLPDC report when it is published in June and consider whether to reflect any of its recommendations in the work
- 'The public core of the Internet' published by the scientific council of the Dutch government. The Public Core of the Internet stands apart as it less an agreement than a research publication. We will encounter its ideas regardless as some of them relate to a GCSC norm.
- ISOC Initiative on Mutually Agreed Norms on Routing Security (MANRS)
- Manila Principles on Intermediary Liability

Both the AU Convention and the Anti-Botnet guide include measures that are undersigned by multiple organizations/states, with the CSDE document being a more technical one with deeper technical practices.

A group of volunteers will be set up to jointly research and develop an initial shared online background paper to narrow down the list of agreements and extract elements from them which will be the focus for the BPF's 2019 report. Prior to publishing anything ahead of our Call for Contributions, this smaller group will bring the document back to the BPF mailing list for review and input. The document will focus on:

- Understanding the context, impact and use of the agreements we plan to investigate this year;
- Identifying unique elements of each agreement and documenting those;
- Performing some basic comparative analysis on what is covered by multiple agreements, and which elements are outliers.

Those that volunteered in response to the call during the meetings and on the list are:

- Sheetal Kumar (Global Partners Digital)
- John Hering (Microsoft)
- Susan Mohr (Century Link)
- Carina Birarda (Buenos Aires Cybersecurity Center – BA-CSIRT)
- Klée Aiken (APNIC)
- José R De La Cruz (ISOC Puerto Rico)
- The lead expert and co-conveners – Maarten van Horenbeeck, Markus Kummer and Ben Wallis

- BPF supporting consultant (IGF Secretariat)

An important step in the work will be to conduct outreach to the organisations responsible for the agreements / initiatives which the BPF decides to explore. This is built into the timeline (see item 4). The BPF will also repeat efforts undertaken in 2018 to inform and get input from the IGF NRIs (national and regional initiatives).

**Item 3) Legal frameworks to explore**

This item related to identifying legal frameworks that the BPF should look at as part of the BPF 2019 output in order to explore what degree they reflect the applicability of international law to the use of ICTs by governments. Volunteers were invited to help with the legal interpretation of these frameworks and see what evidence could be identified regarding the applicability of international law, and it was noted that this invitation would also be posted to the BPF mailing list. There were no comments during the meeting and Maarten will follow up offline with those who had previously expressed interest in this aspect.

**Item 4) High-level timeline for the 2019 BPF Cybersecurity activities**

Ben Wallis set out the steps to be taken throughout the year, culminating in the publication of a final report. A timeline, including indicative dates, can be found below:

- Meeting 1 on scoping the work – March 12 / 20
- Development of initial research papers by team of volunteers – late March to early May
- Meeting 2 to review research papers, take any resulting decisions and begin scoping the public Call for Contributions – Early May
- Launch call for contributions – mid/early May (with deadline of mid-July
- Outreach to specific actors, e.g. signatories to agreements being explored, governments, other key stakeholders – Mid May
- Drafting of BPF report by consultant and engagement where needed to broaden input – mid-July – late August
- Meeting 3 to discuss draft BPF report and planning BPF session at IGF 2019
- Publish draft report ahead of IGF 2019 – by 8th October (6 weeks before IGF 2019)

Meeting participants were asked to note potentially relevant events during the year to be taken into account and the following were suggested:

- WSIS Forum (8-12 April)
- GFCE Council Meeting
- EuroDIG (19-20 June)
- BRICS Summit
- IGF pilot project re Internet security standards – running through the year, culminating in a session at IGF 2019. Wout de Natris is running the project and can keep the BPF informed via the mailing list.