Input from the BPF Cybersecurity to the **Informal Inter-Sessional Meetings of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025.**
December 2022

Input to the Thematic Session Confidence-building Measures:
6 December 2022

Thank you Chair, distinguished delegates for the opportunity to address the OEWG at this intersessional.

I am pleased to present work from the Internet Governance Forum's Best Practice Forum on Cybersecurity. The Best Practice Forum on Cybersecurity is a multistakeholder workstream intersessional of the Internet Governance Forum which brings together a range of experts from all stakeholder groups. For the last three years we have focused on investigating cyber norms development and implementation. Our work showcases the **value of multistakeholder research and capacity building to support States to implement the UN agreed norms.** Research is important to ensure that capacity building is evidence based.

The BPF research in 2020 demonstrated that **the success of cybersecurity norms agreements largely depends on actions by its signatories and stakeholders**. An agreement will facilitate actions if it is clear, defines key terminology, focuses on goals and avoids being overly prescriptive on implementation, makes awareness-raising and capacity-building a crucial part of the agreement, foresees follow-up, monitoring and accountability mechanisms. A lack of leadership in implementation, especially by influential actors, states, or those who called for the agreement, can undermine the success of an initiative.

The BPF in 2021 and 2022 reviewed cybersecurity events, selected based on their coverage in the media, demonstrable harm, successful mitigation and their relation to cyber norms to assess which cyber norms could have been helpful at mitigating impact of the incident, or preventing harm. The investigators found that **the cyber norms we have today would have helped mitigate many of the notorious large cyber incidents of the past**. However, each analysis uncovered **a missing nuance from deeper stakeholder involvement, to application of existing legal frameworks**. The research underscored **the importance of listening to those closest to cybersecurity incidents (e.g. first responders and those directly affected)**, past and present, in order to better mitigate future events. The voices of those most affected by cybersecurity events provide key nuance that are not present in secondary source reports or tertiary source reporting. Our distilled findings point to a gap in understanding the roles of a wide variety of actors and stakeholders in mitigating cybersecurity incidents. And they show a persistent disclarity in the interplay of norms, policies, and laws - which impacts implementation.

To bridge this gap, we recommend future research work that is focussed on **understanding the interplay of cybersecurity norms and legislation including cybercrime legislation, where they overlap align or are not aligned, with an aim to introduce greater stakeholder participation in the creation, enforcement and response mitigation as outlined in cybersecurity norms**. Examples of the incidents analysed and the lessons learned can be accessed on the BPF's website.

The work of the BPF is unique and illustrates the value of multistakeholder engagement, particularly the roles of different stakeholders in socialising norms, supporting their implementation through specific, concrete analysis and ensuring that implementation is evidence-based and informed by their impact on humans. This work will help ensure implementation of the acquis going forward, a key priority for this OEWG, is effective. We encourage member state representatives to take time to engage with the recent outputs of the BPF and follow up with any questions, and we look forward to future opportunities to engage with the OEWG as the process moves forward.

Speaking notes as delivered by Ms Sheetal Kumar, Global Partners Digital, on behalf of the BPF Cybersecurity.

IGF Best Practice Forum Cybersecurity
Recent work on cyber norms agreements

- Draft outputs of the BPF 2022 work cycle
- The Use of Norms to foster Trust and Security (IGF 2021 cycle)
- Exploring Best Practices in Relation to International Cybersecurity Initiatives (IGF 2020 cycle)
- BPF Cybersecurity on International Cybersecurity Agreements (IGF 2019 cycle)
- Cybersecurity Culture, Norms and Values (IGF 2018 cycle)

Input from the BPF Cybersecurity to the **Informal Dialogue with the Chair of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025.** 21 July 2022

IGF Best Practice Forum Cybersecurity webpage
https://www.intgovforum.org/en/content/bpf-cybersecurity

Internet Governance Forum
https://www.intgovforum.org/