IGF Best Practice Forum on Cybersecurity

Kick-off call

Tuesday 2 May 2023

7:00am - 8:00am UTC
AGENDA

1. Welcome & introductions
2. Overview of the BPF Cybersecurity work
3. Plan for 2023
4. Outreach and engagement
5. Next steps
The **Best Practice Form on Cybersecurity** is an IGF intersessional activity to collect existing and emerging good practices from community experience. The bottom-up developed BPF outputs intend to contribute to an understanding of global good practice, and to serve as a resource to inform policy discussions, standards development, business decisions, as well as public understanding, awareness and discourse.
2018  Cybersecurity Culture, Norms and Values and norms development mechanisms.

2019  Cybersecurity norms operationalization best practices
Analysis of commonalities in international and cross-stakeholder cybersecurity initiatives.

2020  Lessons learned from normative principles in global (non-cybersecurity) governance.
Best practices in relation to international cybersecurity agreements.

2021  Understanding the drivers behind cybersecurity initiatives.
Would existing norms have been useful during real-life historical security incidents?

2022  Analysis of frequency and trends of norm elements in cybersecurity agreements.
Storytelling as effective tool to learn from first responders and those most affected by incidents
Ad hoc paper: Mythbusting: Cybercrime versus Cybersecurity
**Timeline**

- BPF Kick-off call: May 2
- Incident Questionnaire: May 16
- IGF 2023 Second Open Intersessional: July 10
- Draft BPF output: September
- IGF Kyoto: October 8-12
- Final BPF output: October 31

---

**BPF Cybersecurity 2023 coordinating team**

**BPF Lead-experts and co-facilitators**
- Mr Klée Aiken
- Mr Bart Hogeveen
- Ms Sheetal Kumar

**IGF MAG co-facilitators**
- Ms Hariniombonana Andriamampionona
- Ms Carina Birarda
- Ms Josephine Miliza

**Supporting consultant IGF Secretariat**
- Mr Wim Degezelle
**Best Practice Forum Cybersecurity - Objectives and work plan for 2023**

**Mandate:**

To collect and evaluate cybersecurity events to present *first-person narratives from those most affected as victims or first responders* to *policy and norms developing deliberations*, so that high-level policy decisions are grounded in reality.

![Diagram showing the relationship between 'Human security' effect, Cybersecurity incident, and Expectations of responsible cyber behaviour (norms).]
Discussion: preferred approach to inform mandate

Idea 1: collect high-profile cases for each region

- Pick 1 incident for each region
- Define impact on:
  - People
  - CI/CII
  - Government services
  - Technical (infra)structure
- Assess effect on observation of norms, and/or implementation

Idea 2: unpack 2-3 high-profile incidents

- Pick two incidents that are publicly well-documented and have affected international stability
- Produce a ‘stereotypical’ timeline for incident and crisis responses, and
- for each phase, determine the effect and impact of international rules & norms, and national cyber policies

Both options driven by crowdsourced analysis from the BPF CS community
Next Steps:

- Collecting potential case studies
  - Utilizing IGF BPF 2022 questionnaire
    - [https://forms.gle/tw5ani54ettw68fM8](https://forms.gle/tw5ani54ettw68fM8)
    - Submit by 16 May 2023
- Shaping the deliverable
- Identifying contributors
Outreach and engagement

Opportunities for the BPF to present its work and plans for 2023

Organisations, experts, forums to invite to the PNIF work streams

Suggestions?

Other IGF intersessional activities (NRIs, DCs)

....
BPF Cybersecurity webpage

www.intgovforum.org/en/content/bpf-cybersecurity

PNIF mailing list

https://mail.intgovforum.org/mailman/listinfo/bpf-cybersecurity_intgovforum.org