IGF 2024

Best Practice Forum

Mainstreaming capacity building for cybersecurity, trust, and safety online

(BPF Cybersecurity Capacity Building)

Call 20 June 2024

Call Summary

Introduction

The *Best Practice Forum on Cybersecurity Capacity Building* is a new best practice forum (BPF) that builds on the work of the BPF Cybersecurty.

Between 2018 and 2023, the BPF Cybersecurity focussed on the development, value and application of cybersecurity norms agreements. More on the BPF Cybersecurity and its outputs can be found here.

The IGF Multistakeholder Advisory Group (MAG) selected cybersecurity capacity building as topic for a BPF during the IGF 2024 cycle. The call on 20 June was the first opportunity to provide feedback on the BPF proposal and discuss scope, focus and work plan for 2024.

The BPF is an intersessional activity of the Internet Governance Forum (IGF) and is open to all interested stakeholders, who are encouraged to join the BPF's mailing list.

Summary of the discussion on the scope and focus for 2024

The participants to the call were invited to comment on the BPF proposal and answer the following two questions :

- *What priorities a BPF on cybersecurity capacity building should focus on?*
- *How to complement and avoid duplication of what is already being done?*

Overall, the BPF proposal was well received; however, several participants who spoke warned that the current idea of mapping cybersecurity capacity-building initiatives risks adding another layer of complexity to an already crowded landscape and could easily duplicate or compete with existing efforts.

The ideas and suggestions made during the following discussion can be grouped into three areas that the BPF could focus on: the duplication of initiatives, the duplication and overlap between initiatives that aim to map and categorise capacity building, and the necessity to explore cyber capacity-building needs concerning new technologies.

Duplication of cybersecurity capacity building initiatives

1. Cybersecurity capacity building can be approached in many ways and cover a wide range of issues. While standardisation is important in today's fast-evolving world, it is also crucial to consider intersectionality.
2. Avoiding overlap and duplication of cybersecurity capacity-building efforts is essential, as it prevents inefficient use of limited funds. The BPF should help identify and understand the issue of duplication in cybersecurity capacity building and contribute to mitigating it.
3. Similarly, it is important to identify where there are gaps and urgent needs.

Duplication of initiatives that map and categorise capacity building

1. Many valuable initiatives already map cybersecurity capacity-building efforts and provide tools to make them accessible to those who need them. For example, the Cybil portal by the GFCE, mapping initiative initiated by the OEWG. The IGF/BPF should avoid duplicating these efforts.
2. Creating a clear overview of who is doing what, where, and with what focus, and potentially fostering cooperation, would be highly valuable, and the IGF/BPF is well positioned to take on this role. Often, there is confusion between initiatives due to a lack of awareness about their different focuses, such as those aimed at UN member states, like in the context of the OEWG, versus those focused on mapping end-user capacity building initiatives. The BPF has an opportunity to clarify these different purposes and as such help to make it easier for the intended target group get access to the right information.
3. Information on cybersecurity capacity-building initiatives in mappings and databases is often scarce, incomplete, or inconsistent due to the different terminologies used by those submitting the information. Because this information comes from various sources, such as governments, implementers, and civil society, it becomes challenging to use effectively. The BPF could highlight this issue.
4. The BPF can highlight good experiences, such as the efforts of UNIDIR and the Cybil Portal to facilitate their data exchange, and explore practical ways to make it easier for target users to find and access the right information.

Awareness raising and capacity building on cybersecurity threats related to new technologies

1. Cybersecurity capacity building and new technology present a broad field. If the BPF is to address this topic, it is crucial to clearly define the focus from the outset.
2. While new technologies provide opportunities to enhance cybersecurity, they also introduce new risks, such as those posed by AI, and the challenge of mitigating them. This creates two distinct needs for capacity building: developing the ability to use new technologies in cybersecurity and building capacity to understand, evaluate, and mitigate the cybersecurity risks associated with these technologies.
