IGF 2024

Best Practice Forum

Mainstreaming capacity building for cybersecurity, trust, and safety online

(BPF Cybersecurity Capacity Building)

Call 26 September 2024

Call Summary

Introduction

The IGF Multistakeholder Advisory Group (MAG) selected cybersecurity capacity building as topic for a Best Practice Forum (BPF) during the IGF 2024 cycle (BPF proposal).The BPF on Cybersecurity Capacity Building builds on the work of the BPF Cybersecurity that, between 2018 and 2023, focussed on the development, value and application of cybersecurity norms agreements (the 2023 and earlier outputs can be found here).

The BPF Cybersecurity Capacity Building held an initial discussion on its scope, focus and work plan for 2024 (call summary). Insights from that meeting contributed to the development of a draft outline for the 2024 work, which was presented in this meeting.

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

During the call on 20 June, participants highlighted that overlap, duplication, and gaps in cybersecurity capacity building lead to inefficient use of limited resources. They agreed that there's no need for the BPF to create another mapping of initiatives, as many valuable efforts already exist—such as the Cybil portal by GFCE, UNIDIR cyberportal, and the Global Cyber Security Capacity Centre. However, there is a lack of a comprehensive overview showing who is doing what, where, and with what focus and purpose. Providing such an overview is important to avoid redundancy among these mapping efforts. Enhanced cooperation and information exchange between existing initiatives could yield significant benefits.

Building on these insights, the BPF designed a draft methodology which includes the following steps:

1. **Defining the Issue**: Clearly articulate the problem of overlap in cybersecurity capacity building efforts and its negative consequences.
2. **Compiling an Overview of Existing Mappings**: Gather and categorise current mappings and inventories of cybersecurity capacity building initiatives by focus areas, topics, target users, and other relevant criteria.
3. **Collecting Case Studies**: Assemble case studies showcasing cooperation and coordination between different mappings and inventories to extract lessons on perceived benefits and obstacles.
4. **Preparing Draft Conclusions and Recommendations**: Develop preliminary conclusions and actionable recommendations based on the findings, to be discussed at the BPF session during IGF 2024.

Feedback on the methodology & draft outline and further Suggestions:

- Global collaboration to share experiences and best practices in cybersecurity capacity building is important.
- Accessible tools and shared knowledge help countries with limited budgets to face capacity building challenges.
- The BPF work should include both global and regional resources.
- ECSO's Road 2 Cyber to be included in the resources.
- As part of the effort to identify overlaps and duplications among existing initiatives, the BPF could look into creating a taxonomy to standardise concepts and terminologies used across different mappings/inventories.
- Suggestion to reach out to and involve academic institutions, regional groups and organisations, such as those in the Pacific and the Americas, and experts.

Next steps:

- Involving more organisations and experts: participants to reach out to their networks.
- Share the draft outline with the BPF mailing list and solicit feedback.
- Developing a data collection form to collect detailed information on existing mappings and inventories.