IGF 2022
Best Practice Forum on Cybersecurity
Executive summary

December 2022

IGF2022 BPF Cybersecurity outputs
https://www.intgovforum.org/en/filedepot_download/56/24125

Introduction

To enrich the potential for Internet Governance Forum (IGF) outputs, the IGF has developed an intersessional programme of Best Practice Forums (BPFs) intended to complement other IGF community activities.

Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics. In the last four years, the BPF on Cybersecurity started investigating the concept of *culture, norms and values in cybersecurity*.

In 2018 the BPF took a closer look at norms development mechanisms. In 2019, when the BPF ran in conjunction with the initiation of UN GGE and OEWG, the BPF looked at best practices related to the operationalization of cyber norms and started analysing international and cross-stakeholder cybersecurity initiatives for commonalities. In 2020, the BPF took a wider approach and explored what can be learned from norms processes in global governance in areas completely different than cybersecurity, and continued and further advanced the analysis of cyber norms agreements. Last year's BPF Cybersecurity investigated more deeply the drivers behind, and disablers of, cyber norms. A second work stream tested norms concepts against historical Internet events to understand how specific norms have or would have been effective at mitigating adverse cybersecurity events.

In 2022, the BPF Cybersecurity added new agreements to its assessment of normative cybersecurity agreements, explored the value of storybanking cybersecurity incidents, and produced an ad hoc mythbusting paper on the difference between cybercrime and cybersecurity from a policy perspective.

Work Stream I - Mapping International Cybersecurity Norms Agreements

The BPF added two new agreements - *the Copenhagen Pledge on Tech for Democracy* and *A Declaration for the Future of the Internet* - to its database, which now includes 38 international agreements between or among stakeholders, including voluntary, nonbinding cybersecurity norms. The analysis showed that “human rights” and “general cooperation” are the most commonly seen norms elements across the 38 agreements. Norms that relate to express restraint on what either government actors, private sector actors, or other actors will not do occur the least frequently, but have become more prominent over time. Interestingly, the new norms agreements included in the 2022 analysis have overlapping qualities as well as norms elements that set them apart. They are both led independently by foreign ministries and have emphasis on protecting democracy and on working to building democratic coalitions, of governments in one case and of broader multistakeholder actors in the other. There’s a focus in both agreements on disinformation, misinformation, and influence operations related to the security of democracies. Lastly, the overall analysis of the 38 agreements showed a growing interest in combating ransomware as an action item.

Work Stream II - Exploring Historic Cybersecurity Events

Building on its work in 2021 that revealed a gap in understanding the roles of actors and stakeholders in mitigating cybersecurity incidents, the work stream 2 explored how storytelling can be an effective tool to listen and learn from the experiences of first responders and those most affected by a cybersecurity event. These insights are valuable input for those involved in cyber norm development. At the end of the day, cybersecurity norms must make a difference in the lived experiences of these people, past, present and future. The workstream 2 developed a framework for collecting stories from networks of first responders.

Work Stream III - Outreach and Engagement

Under its Outreach and Engagement work stream the BPF organised an outreach session during *RightsCon 2022* and contributed relevant findings of its work on cybersecurity norms with the *UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025* during the OEWG Chair’s Informal Dialogue (BPF input) and Informal Inter-Sessional Meetings (BPF input).

Ad hoc paper - Mythbusting: Cybercrime versus Cybersecurity

The BPF created an ad hoc work stream to develop a paper to help stakeholders understand the key policy differences between cybersecurity and cybercrime such that their advocacy strategies can better align with a human rights centric approach to internet governance. In general the suggested strategy is to remove the policy decision making out of the criminal frameworks so as to balance the implications on human rights, while promoting cybersecurity as an incentivized, normative framework that depends on cross sector collaboration, and can be compatible with human rights. The paper is available online.