IGF 2021

Best Practice Forum Cybersecurity

on the use of norms to foster trust and security

Draft findings of the BPF on Cybersecurity 2021

The 2021 BPF on Cybersecurity has continued work to support the ongoing development of cybersecurity norms in the UN and elsewhere. Two weeks ahead of the IGF in Katowice, and our final meeting of the year, we are publishing two draft papers to support these ongoing discussions. In our research product this year, we have worked to identify relevant cybersecurity norms agreements and investigated more deeply the drivers behind, and disablers of, cyber norms. The BPF also researched major historical cybersecurity incidents, with as goal to understand how they can help drive further norms discussions; and help us understand which norms would have been useful during their mitigation.

Mapping and Analysis of International Cybersecurity Norms Agreements

Recent years have witnessed a persistent escalation of sophisticated attacks in cyberspace, resulting in the rapid emergence of a new domain of conflict. As with other domains of conflict, expectations for responsible behavior to promote stability and security have necessarily started emerging as well in the form of multilateral, regional, and bilateral agreements between states on voluntary and non-binding norms of conduct. The BPF included 36 such agreements in this year's study, which each:

- Describe specific commitments or recommendations that apply to any or all signatory groups (typically governments, non-profit organization or private sector companies);
- Define commitments or recommendations in the agreement must have a stated goal to improve the overall state of cybersecurity;
- Are international in scope – intended to apply multiple well-known actors that either operate significant parts of internet infrastructure or are governments and therefore representing a wide constituency.
- Include voluntary, nonbinding norms for cybersecurity, among and between different stakeholder groups.

Our draft report provides deeper analysis of each agreement, but specifically noted the following findings of interest regarding the focus of cyber norms:

- When it comes to the most prominent norm elements reflected across all agreements, considerations surrounding (4.1) “general cooperation” and (1.1) “human rights” were the most frequently included norm elements.
- The emphasis on human rights across agreements is especially notable because not only is it the second most frequently recognized norm element, but also because this recognition has been consistently and noticeably growing over time.
- The two least frequently cited norm elements across all agreements included were both in the fifth norm category: “Restraint on the development and use of cyber capabilities”.

Testing norms concepts against historical internet events

The BPF then focused on understanding the answer to the question “*How would specific norms have been effective at mitigating adverse cybersecurity events?*”. This was done through a detailed review of nine major cybersecurity events, selected based on their coverage in the media, demonstrable harm, successful mitigation and their relationship to cyber norms. These events included incidents such as Ghostnet, Stuxnet, NSO Group’s Pegasus and Solarwinds.

For each of these incidents, a group of expert contributors sought to answer the central research question through desk research and analysis. In each case, an assessment is provided on 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 cyber events of the past. However, each analysis uncovered a missing nuance from deeper stakeholder involvement, to application of existing legal frameworks. For instance, the case of the GhostNet event of 2009 highlighted that cyber resilience should be a community-level concern that when addressed at the hyperlocal level, lends capacity to at-risk groups to shift into monitoring mode and can respond to the evolution of threats over time.

Drafts available for comment

Drafts of both research papers are now available for input, ahead of the BPF on Cybersecurity meeting in Katowice, on December 10th, 2021.

Mapping and Analysis of International Cybersecurity Norms Agreements
Draft Report, November 2021

Testing norms concepts against cybersecurity events
Draft Report, November 2021

Submit comments via bpf-cybersecurity-info@intgovforum.org .

BPF Cybersecurity Main session at IGF 2021

BPF Cybersecurity Main session at IGF 2021, Friday 10 December, 10:15-11:45 UTC.