IGF 2019

Best Practice Forum on Cybersecurity

Cybersecurity Agreements

Executive Summary

The 2019 work track of the IGF Best Practice Forum on Cybersecurity identified spaces of norms development across the global community and collected best practices on how signatories put cybersecurity agreements into actions.

The BPF Cybersecurity is one of the core intersessional activities of the Internet Governance Forum (IGF) initiated since 2014. It provides a platform for focused multistakeholder discussion on cybersecurity policy challenges with the intent to inform internet governance policy debates by drawing on the immense and diverse range of experience and expertise found in the global IGF community.

The BPF analyzed twenty different cybersecurity agreements - including the Paris Call for Trust and Security in Cyberspace and the UNGGE 2015 consensus report - and discussed the purpose, value and outcome of those agreements, as well as collecting examples of stakeholder actions that support achieving an agreement's goals.

Cybersecurity agreements and norms initiatives

Cybersecurity agreements have the ambition of being important milestones and substantive contributions to improving cybersecurity. They have their own scope and focus, which can be broad

or specific, and promote a certain expected behaviour in cyberspace that is, its signatories agree, beneficial to cybersecurity.

Cybersecurity agreements contribute to establishing cybersecurity norms. Norms are most commonly defined as collective expectations for what is seen as proper behaviour for an identifiable group, and express an aspiration to act accordingly or restrain from improper behaviour. Norms derive their strength from the fact that they are internalised and valued by a community and, unlike rules, do not need to be imposed or enforced. When an actor feels a need to hide behaviour, deny or lie about it, or puts special effort into mapping and demonstrating certain behaviour, it is often an indication that something has become a norm.

Perceived value and outcome of cybersecurity agreements

As threats in cyberspace are becoming more commonplace and severe, cybersecurity agreements provide a valuable common footing to reduce risk and increase security and stability in cyberspace. The agreement's text, with its substantive content and goals, is a tangible and valuable document, and often the outcome of a long process with different parties involved. Both the process, which may bring stakeholders closer to each other and increase trust, and its product, 'the Agreement', are valuable. The accompanying announcement and communication efforts may contribute to spreading awareness and knowledge about the cybersecurity issue(s) addressed to a wider audience.

The BPF concluded that cybersecurity agreements may:

- develop and reinforce clear expectations for reasonable behaviour;
- clarify responsibilities, create obligations and trigger more active accountability for identifiable actors;
- contribute to the visibility and promotion of good cybersecurity practices;
- operate as confidence-building measures between stakeholders and facilitate further cooperation;
- facilitate the development of new relationships and partnerships, in particular when multistakeholder participation is allowed.

Unintended and adverse effects of cybersecurity agreements

Notwithstanding the good intentions of signatories and stakeholders, cybersecurity agreements may remain ineffective or even provoke adverse and counterproductive effects. These unintended outcomes can often be traced back to causes within the agreement, the process and course of actions that lead to the agreement, or reasons and challenges within a broader context. A typical example is the lack or late involvement of stakeholders whose actions will be instrumental for obtaining the goals of the agreement.

The BPF found that cybersecurity agreements are at risk of becoming counterproductive to furthering cybersecurity when they:

- limit multistakeholder input;
- fail to focus on outcomes but instead prescribe a particular course of action;
- miss the involvement of certain important global players;
- lack leadership in implementation;
- directly or indirectly undermine human rights, which in turn may reduce cybersecurity.

Improving the quality of cybersecurity agreements

The success of a cybersecurity agreement largely depends on actions by its signatories and stakeholders to pursue the goals of the agreement. Implementers of agreements may face a number of challenges that delay or prevent them from taking action. The quality of the agreement and its ability to substantially contribute to improving cybersecurity may be increased by foreseeing and addressing these challenges early on. The BPF identified a number of challenges and formulated the following suggestions to improve the quality of cybersecurity agreements:

- Define key terminology early in the agreement.
  Varied understandings of definitions of key terminology referred to in the agreement may hinder the cooperation amongst signatories and stakeholders.

- Be clear and unambiguous.
  Vague and ambiguous language of an agreement may require further negotiation and clarification before action can be taken. Agreements should strive to provide a sufficient enough balance in guidance on how to implement an agreement and clarity on the respective roles and responsibilities required.

- Focus on goals and avoid being overly prescriptive on implementation.
  Overly prescriptive agreements that strictly determine how actors should implement various provisions risk being less effective. Allowing stakeholders the flexibility to choose the approach to pursue the goals of the agreement that best fits their situation or context is a strength.

- Make awareness-raising and capacity-building a crucial part of the agreement.
  Varied levels of awareness of the existence of an agreement and varied knowledge and capacity to take action and implement may explain why some agreements remain without further action.

- Foresee follow-up, monitoring and accountability mechanisms.
  The lack of continuity once an agreement has been reached or published, and the abrupt discontinuation of consultation processes or interactions between stakeholders may take

away the momentum. A lack of institutional capacity and mechanisms to monitor compliance and implementation does not incentivise responsible behaviour. Sharing of experiences and case studies of how stakeholders implement parts of the agreement can motivate and help other stakeholders to learn from peers and identify good practices.

It was also flagged that a lack of leadership in implementation, especially by influential actors, states, or those who called for the agreement, can undermine the success of an initiative.

Importance of multistakeholder involvement

Only a relatively small number of agreements have so far been developed within clear multistakeholder spaces. Including stakeholders in the design of norms and agreements can avoid needless ambiguity and the need to clarify language afterwards. It happens that stakeholders are invited to the discussions near the end of the process, which is too late for them to weigh in and ensure that agreements can be implemented.

It is important that actors are given the opportunity to share how they are approaching the commitments and their implementation to allow for others to learn from peers and identify good practices. Building networks, such as Communities of Interest, as proposed by the Global Commission on the Stability of Cyberspace, where stakeholders can cooperate on implementation, can be very valuable.

Civil Society has taken a leading role in assessing adherence to norms and as such contributed to establishing accountability and enumeration of responsible behaviour. This engagement can be a basis for other multistakeholder approaches.

Concluding remarks

The uprise of different norm initiatives is not a bad sign. They are filling gaps where more binding policy measures are not possible because there is a lack of a collective understanding of what the issues are and no agreement among stakeholders on what the adequate solutions are. However, there are the beginnings of consensus expectations that across different initiatives can become a common basis to build on. This process best focuses on what has to be done (identify the common goals) and requires the creativity that only multistakeholder and multidisciplinary collaboration can bring to the table.

The BPF Cybersecurity had the opportunity to present its work at the United Nations' Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security during the OEWG's informal intersessional consultative meeting with industry, non-governmental organizations and academia on 2-4 December 2019 at the UN headquarters in New York.

IGF2019 BPF Cybersecurity

IGF2019 BPF Cybersecurity full report (.pdf)
BPF webpage https://www.intgovforum.org/multilingual/content/bpf-cybersecurity
BPF workshop at IGF2019, Berlin: agenda & report / recording

End of document