Submission to the ‘Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.’

*February 2020*

**Abstract**

As a forum for multistakeholder policy dialogue, the Internet Governance Forum (IGF) is mandated to discuss Internet public policy issues, identify and deliberate emerging issues and facilitate the exchange of information and best practices. *Security* was one of the key themes of the IGF and has been discussed in various forms dating back to 2006 when the IGF held its first meeting. Security remains as a recurring theme for its past session, including at its recent 14th meeting in Berlin on 25-29 November 2019, hosted by the Government of Germany.

This submission intends to provide the OEWG with information, insights and recommendations that came out of the exchanges among stakeholders (that include Governments, the Internet technical community, private sector, civil society, and international and regional organizations) in the context of Internet governance that are related to and might be relevant for its current deliberations. While this contribution is mainly reporting on work done in the context of the IGF 2019, as mentioned, the IGF represents a rich resource of documented discussions on policy issues related to key elements of Internet governance, including norms, best practices and capacity development initiatives. All resources are available online ([IGF website](https://www.igfuzz.com)).
Messages of the IGF 2019 on Cybersecurity

IGF Messages capture the main policy trends and discussions across the different meetings during the annual forum as well as its intersessional activities. Several messages of the IGF 2019 in Berlin are directly related to the issues discussed by the OEWG, in particular the messages recorded under the Security, Safety, Stability and Resilience thematic track.

Policy and Cooperation

The IGF 2019 messages convey that 'the future of the Internet is a shared responsibility. Multistakeholder and multidisciplinary dialogues are the most appropriate ways to find policy solutions and to identify physical world implications of behaviour and policy decisions in the online space'.

Multistakeholder dialogue in the area of cybersecurity has the potential to evolve into consensus building and effective and predictable policy implementation. To make full use of these opportunities, it is important to develop 'deeper understandings of the different roles that different stakeholders can take in discussions and the identification of possible solutions' to cybersecurity challenges. To facilitate the dialogue, it is recommended to 'standardize definitions and terms' and to ensure meaningful participation of all stakeholders, including by avoiding too many parallel discussions on the same issues.

The IGF Messages acknowledge the importance of cybersecurity norms and norms development and stress that 'every effort to pursue what is considered proper behaviour contributes to establishing community-wide supported cybersecurity norms.'

Capacity Building

‘There are various forums, including the IGF, and initiatives for multilateral, regional and bilateral engagement, where states can build up relationships, exchange experiences and learn from innovative new approaches.’

The IGF Messages highlight the importance for improved cybersecurity of fostering ‘a more informed dialogue between stakeholders, based on a better understanding of the technical, legal and economic feasibility of the various digital sovereignty models being considered or implemented around the world as well as their implications for Internet governance’.

Capacity building for policy makers and stakeholders and initiatives that promote trust between states and stakeholders contribute to the global security ecosystem. It is important to empower users, including vulnerable groups and minorities, and countries with special needs, including countries with transition economies, least developed countries, landlocked developing countries and small island developing states. All users have an obligation to contribute to
security on the Internet, but ‘they can only be expected to act as responsible users if they understand what is at stake, are aware of the risks, know their rights, and have learned how to act’.

**Safety and Security online**

‘The Internet will only achieve its potential as a channel of free speech and an engine for economic growth if it remains a safe place where people feel secure.’ Different sessions at IGF 2019 covered different aspects of online safety and security, including tackling hate speech, disinformation and interference of electoral processes, the protection of children’s rights, and addressing illicit and abusive content. The IGF messages underline that it is important that ‘discussions on online safety need to rely on robust data’, and that the ‘international multistakeholder community needs to accurately define scope and terminology’ and develop a ‘shared understanding amongst all players’ as a basis for agreement on ways to act and cooperate.

The full set of *Messages of the IGF 2019* can be found on the IGF website at [https://www.intgovforum.org/multilingual/content/berlin-igf-messages](https://www.intgovforum.org/multilingual/content/berlin-igf-messages)

**IGF 2019 Best Practice Forum on Cybersecurity**

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 has been one of the core intersessional activities of the IGF since 2014. It provides a platform for focused multistakeholder discussion. The BPF analyzed nineteen 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. The BPF had the opportunity to report on its key findings at the OEWG’s international consultative meeting in December (for reference, see the [contribution of the IGF BPF Cybersecurity to the OEWG consultative meeting](https://www.intgovforum.org/multilingual/content/berlin-igf-messages)).
Key Findings of the BPF Cybersecurity

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 led 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 can be the case 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 behaviours. This engagement can be a basis for other multistakeholder approaches.

BPF Cybersecurity 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 adequate solutions. However, there are the beginnings of consensus expectations that, across different initiatives, that 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.

Links and Report of IGF 2019 BPF Cybersecurity

- IGF 2019 BPF Cybersecurity ‘Cybersecurity Agreements’ – full report
  The report includes the mapping analysis of 19 international cybersecurity agreements examples of projects and actions by signatories and stakeholders implementing the agreements.
About the Internet Governance Forum
The IGF serves to bring people together from various stakeholder groups as equals, in discussions on public policy issues relating to the Internet. While there is no negotiated outcome, the IGF informs and inspires those with policy-making power in both the public and private sectors. At their annual meeting delegates discuss, exchange information and share good practices with each other. The IGF facilitates a common understanding of how to maximize Internet opportunities and address risks and challenges that arise.

About the IGF Messages
IGF Messages have been compiled since the IGF meeting in 2017. They provide policy makers with a quick and high-level overview of policy trends drawn from the discussions at the annual meeting. The Messages are compiled and updated throughout the IGF week with draft versions published on the IGF website for the consideration and input of participants.

About the IGF Best Practice Forums
IGF Best Practice Forums (BPFs) are part of the IGF’s intersessional work programme that was introduced in 2014 with the objective to strengthen the IGF and make it more relevant. BPFs intend to inform Internet governance policy debates by drawing on the immense and diverse range of experience and expertise found in the global IGF community to create a resource of best practices and policy recommendations. Since 2014 BPFs have been convened on a variety of topics to discuss best practices and compile output reports in an open and bottom-up process. There have been BPFs on, amongst others, cybersecurity, IPv6, gender and access, local content, online child protection, and IoT, Big Data, AI. A repository of BPF reports is available on the IGF website.

Please contact IGF Secretariat for any queries:
United Nations
Secretariat of the Internet Governance Forum (IGF)
Villa Le Bocage
Palais des Nations,
CH-1211 Geneva 10
Email: igf@un.org
Phone: +41 (0) 229 173 411