****

**Call for Contributions on the 2019 BPF on Cybersecurity**

The IGF Best Practices Forum on Cybersecurity is a multistakeholder group focusing on identifying best practices in Cybersecurity. From [2016-2018](https://www.intgovforum.org/multilingual/content/best-practice-forums-bpfs), the group has focused on identifying roles and responsibilities of individual stakeholder groups in cybersecurity, and investigated the development of culture, norms and values in cybersecurity.

In 2019, the BPF Cybersecurity is focusing on international agreements and initiatives on cybersecurity. The main objective of this year's effort is to identify best practices related to the implementation, operationalization, and support of different principles, norms, and policy approaches contained in these international agreements/initiatives by individual signatories and stakeholders. initiatives. Amongst others, these agreements include for instance the [Paris Call for Trust and Cybersecurity in Cyberspace](https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf), the [Tech Accord](https://cybertechaccord.org/accord/), the Shanghai Cooperation Organization’s [Agreement on cooperation in the field of ensuring the international information security](http://eng.sectsco.org/load/207508/) and the [2015 UNGGE proposed norms](https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).

The IGF Best Practices Forum on Cybersecurity is calling for input for its 2019 effort[[1]](#footnote-1).

For a better understanding of the types of agreements we are investigating, we recommend reading the [background paper published by the BPF Cybersecurity](https://www.intgovforum.org/multilingual/filedepot_download/4904/1658). and available [here (.pdf)](https://www.intgovforum.org/multilingual/filedepot_download/4904/1658) . The paper provides an overview of international agreements and initiatives by focusing on the (i) identification of spaces for agreement, (ii) assessment of the state of existing agreements and (iii) next steps for implementation.

Please find below the list of questions. We recommend that, when *possible* and *applicable*, contributors refer to the list of initiatives outlined in Annex A.

|  |
| --- |
| **Instructions.**  **Please attach contributions as Word Documents (or other applicable non-PDF text) in an e-mail and send them to** [**bpf-cybersecurity-contribution@intgovforum.org**](mailto:bpf-cybersecurity-contribution@intgovforum.org) **.** You’re kindly requested to try to keep the contributions to **no more than 2-3 pages**, and to include URLs/Links to relevant information.  Contributions will be published on the [BPF webpage](https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-2019-contributions) and included in the BPF’s output document. Please inform us here, should there be any limitations on the publication of your contribution, and indicate what title, organisation or contact person could be used to identify your contribution.  **Deadline**: the BPF accepts contributions and input on a rolling basis. Contributions received by Sept 20 will be included in the draft BPF report published before the IGF meeting. Contributions after Sept 20 will be posted on the BPF webpage and serve as input for the BPF discussions before and at IGF2019 in Berlin. They will be incorporated in the final BPF output report. |

**Questions**

1. Is your organization a signatory to any of the agreements covered, or any other ones which intend to improve cybersecurity and which our group should look at? If not, we are still interested in your opinion on the rest of this questionnaire!
2. What projects and programs have you implemented or have seen implemented to support the goals of any agreements you signed up to? Do you have any plans to implement specific projects?
3. During [our review,](http://www.intgovforum.org/multilingual/filedepot_download/4904/1658) we identified a few key elements that were part of multiple agreements and seem to have more widespread support and/or implementation. Do you have views around the relative importance of these (e.g. by providing a ranked list), or are there any others that you consider to be significant commitments in these types of agreements?   
   * **Furthers multi-stakeholderism:** identify or support that cybersecurity depends on the presence in debate and coordination of all stakeholder groups.
   * **Vulnerability equities processes:** the realization that stockpiling of vulnerabilities may reduce overall cybersecurity, and processes can be implemented to help identify the appropriate course of action for a government when it identifies a vulnerability.
   * **Responsible disclosure:** the need to coordinate disclosure of security issues between all stakeholders, including the finder, vendor and affected parties.
   * **Reference to International Law:** whether the agreement reflects on the importance of aligning international law.
   * **Definition of Cyber threats:** whether the agreement proposes a clear or aligned definition of cyber threats.
   * **Definition of Cyber-attacks:** whether the agreement proposes a clear or aligned definition of cyber attacks.
   * **Reference to Capacity Building:** whether the agreement makes specific references to Capacity Building as a needed step to improve cybersecurity capability.
   * **Specified CBM’s:** whether the agreement describes or recommends specific Confidence Building Measures.
   * **Reference to Human Rights:** whether the agreement reflects on the importance of human rights online.
   * **References to content restrictions:** whether the agreement discusses the need for content restrictions online.
4. What has the outcome been of these agreements? Do you see value in these agreements either as a participant, or as an outsider who has observed them?
5. Have you seen any specific challenges when it comes to implementing the agreement?
6. Have you observed adverse effects, or tensions from any of the elements of these agreements, where specifics may be at odds with intended end results? For instance a commitment that may seem like it improves cybersecurity at first sight or tries to fix one issue, but has effects that lead to a reduction in cybersecurity?

**Annex A: List of agreements for consideration**

* The G20, in their [Antalya Summit Leaders’ Communiqué](http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/), noted that “affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors”.
* The G7, in their [Charlevoix commitment on defending Democracy from foreign threats](https://www.mofa.go.jp/files/000373846.pdf), committed to “Strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state.”
* The [Cybersecurity Tech Accord](https://cybertechaccord.org/accord/) is a set of commitments promoting a safer online world through collaboration among technology companies.
* The Freedom Online Coalition's [Recommendations for Human Rights Based Approaches to Cyber security](https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf) frames cyber security approaches in a human rights context, and originates from a set of member governments.
* In the Shanghai Cooperation Organization’s [Agreement on cooperation in the field of ensuring the international information security](http://eng.sectsco.org/load/207508/) member states of the Shanghai Cooperation Organization agree on major threats to, and major areas of cooperation in cybersecurity.
* The [African Union Convention on Cyber Security and Personal Data Protection](https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection) assists in harmonizing cybersecurity legislation across member states of the African Union.
* The Council to Secure the Digital Economy is a group of corporations which together published an [International Anti-Botnet guide](https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf) with recommendations on how to best prevent and mitigate the factors that lead to widespread botnet infections.
* The League of Arab States published a [Convention on Combating Information Technology Offences](https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection) which intends to strengthen cooperation between the Arab States on technology-related offenses.
* Perhaps one of the oldest documents, the Council of Europe developed and published a [Convention on Cybercrime](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185), also known as the Budapest Convention. Adopted in November 2001, it is still the primary international treaty harmonizing national laws on cybercrime.
* The East African Community (EAC) published its [Draft EAC Framework for Cyberlaws](http://unctad.org/en/pages/PressReleaseArchive.aspx?ReferenceDocId=13379) in 2008, which contains a set of recommendations to its member states on how to reform national laws to facilitate electronic commerce and deter conduct that deteriorates cybersecurity.
* The Economic Community of Central African States (ECCAS) in 2016 adopted the [Declaration of Brazzaville](http://www.ceeac-eccas.org/images/PDF/DISCOURS/DeclarationDeBrazzaville24Nov16.pdf), which aims to harmonize national policies and regulations in the Central African subregion.
* The Economic Community of West African States (ECOWAS) [Directive C/DIR. 1/08/11](http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf) on Fighting Cyber Crime within ECOWAS, agree with central definitions of offenses and rules of procedure for cybercrime investigations.
* The European Union in 2016 adopted, and in 2018 enabled its [Directive on Security of Network and Information Systems (NIS Directive).](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN) The Directive provides legal measures to improve cybersecurity across the EU by ensuring states are equipped with incident response and network information systems authorities, ensuring cross-border cooperation within the EU, and implement a culture of cybersecurity across vital industries.
* In December of 2018, the EU reached political agreement on a [EU Cybersecurity Act,](http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf) which reinforces the mandate of the EU Agency for Cybersecurity (ENISA) to better support member states. It also built in a basis for the agency to develop a new cybersecurity certification framework. In May 2019, the EU adopted and authorized the use of [sanctions in response to unwanted cyber-behavior](https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/).
* The NATO Cyber Defence Pledge, launched during NATO’s 2016 Warsaw summit, initiated cyberspace as a fourth operational domain within NATO, and emphasizes cooperation through multinational projects.
* In 2017, the EU Council published to all delegations its conclusions on [the Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.](https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Bilateral/EU+Council+Conclusions+on+the+Joint+Communication+Resilience%2C+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU.pdf) This reinforced several existing EU mechanisms, such as the EU Cyber Security Strategy, and further recognized other instruments such as the Budapest Convention, while calling on all Member States to cooperate on cybersecurity through a number of specific proposals.
* The [Mutually Agreed Norms for Routing Security (MANRS)](https://www.manrs.org/), an initiative by the Internet Society, is a voluntary set of technical good common practices to improve routing security compiled primarily by members of the network operators community.
* The[Southern African Development Community Model Laws on Cybercrime](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf)were developed with the intent of harmonizing ICT policies in sub-saharan Africa.
* The[Paris Call for Trust and Security in Cyberspace](https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf)**,** launched by France at the 2018 IGF, currently has 547 official supporters, including 65 states.
* [UNGGE Consensus Report of 2015](https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174)
* The[Siemens Charter of Trust](https://new.siemens.com/global/en/company/topic-areas/digitalization/cybersecurity.html)contains several product development norms, such as “user-centricity” and “security by default”
* [GCSC Six Critical Norms](https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf) **-** At the time of writing, the six critical norms are still in draft, and published for public input.

1. **Deadline**: the BPF accepts contributions and input on a rolling basis. Contributions received by Sept 20 will be included in the draft BPF report published before the IGF meeting. Contributions after Sept 20 will be posted on the BPF webpage and serve as input for the BPF discussions before and at IGF2019 in Berlin. They will be incorporated in the final BPF output report. [↑](#footnote-ref-1)