

**IGF 2020**

**Best Practice Forum Cybersecurity**

**CALL FOR CONTRIBUTIONS**



**Introduction**

The [IGF Best Practice Forum on Cybersecurity](https://www.intgovforum.org/multilingual/content/bpf-cybersecurity) is a multistakeholder group focusing on identifying best practices in Cybersecurity.

Last year, the BPF published [research](https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-2019) to identify best practices related to the implementation, operationalization, and support of different principles, norms, and policy approaches contained in these international agreements and initiatives by individual signatories and stakeholders. Amongst others, these agreements include 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 [Agreement on cooperation in ensuring the International Information Security between the Member States of the Shanghai Cooperation Organization](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). **In 2020, the BPF Cybersecurity is building on its 2019 report by focusing on identifying additional international agreements and initiatives on cybersecurity, and performing a deeper analysis of a narrower set of agreements.** In this deeper analysis, we’re looking specifically at whether the agreement includes any of the UN-GGE consensus norms; and whether any additional norms are specifically called out. The narrower set of agreements is focused on those that are specifically normative, rather than having directly enforceable commitments.

**Instructions:**

The Best Practice Forum on Cybersecurity is calling for input for its 2020 effort. Input will feed into the BPF discussions, the BPF workshop during the virtual IGF2020 and this year’s BPF output report.

We are soliciting input by October 17th, 2020.

Contributions can be submitted to [bpf-cybersecurity-contribution@intgovforum.org](mailto:bpf-cybersecurity-contribution@intgovforum.org) . (download a word version of the call here)

Contributions will be published on the BPF webpage, feed into the BPF discussions at IGF2020 and BPF output report.

**Background reading :**

For a better understanding of the types of agreements we are investigating, we recommend reading the research paper prepared by the BPF’s workstream 1: [Exploring Best Practices in Relation to International Cybersecurity Agreements](https://www.intgovforum.org/multilingual/filedepot_download/10387/2253) (.pdf).

If you’re interested in the broader topic of norms development and norms assessment in global governance, we recommend the excellent background paper ‘[What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance](https://www.intgovforum.org/multilingual/filedepot_download/10387/2252)’ (.pdf) published by the BPF’s workstream 2.

CALL FOR CONTRIBUTIONS

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.

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? *(please indicate the name(s) of the agreement(s), and, in case the agreement is not yet covered by the BPF (see Annex A), provide details in question 3)*
2. What projects and programs have you implemented to support norms agreements your organization has agreed with?
3. Are you aware of any other cybersecurity agreements that describe specific norms in cyberspace? If so, could you provide the following information?
   * Name of agreement
   * Date of launch
   * Stakeholders party to the agreement
   * Number or link to list of signatories
   * Which organization maintains the agreement? If possible, provide contact information
   * Does the agreement include any of the following UN-GGE consensus norms?
     + States should not allow territory be used for international wrongful acts via ICTs
     + Do not conduct or support ICT activity that harms critical infrastructure.
     + Protections for ICT supply chain security, preventing the spread of malicious ICT tools.
     + Recognizing computer emergency response teams as a protected and benign group.
     + Recognizing human rights online and/or right to privacy
     + Cooperation with states to increase stability and security in use of ICTs
     + States (or other stakeholders) should consider all relevant information following ICT incidents
     + States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs
     + States (or other stakeholders) should protect their own critical infrastructure
     + States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack
     + Encourage responsible reporting of ICT vulnerabilities and share remedies
4. Are there cybersecurity issues you believe should be addressed by a cybersecurity agreement which are currently not?
5. We welcome your comments and thoughts ! Feel free to use this call for contributions to share general observations on the topic, provide feedback on the BPF's background paper '[What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance](https://www.intgovforum.org/multilingual/filedepot_download/10387/2252)', the BPF's draft research paper '[Exploring Best Practices in Relation to International Cybersecurity Agreements](https://www.intgovforum.org/multilingual/filedepot_download/10387/2253)', or to suggest ways forward for the BPF in 2021.

**About you (should you be willing to share this information)**

*Case studies will be published online and as part of the BPF output report. We would welcome your contact details to be able to reach out to you for additional information. (email addresses will not be published) You are welcome to remain anonymous should you prefer to do so.*

Name

Affiliation

E-mail (for contact only/will not be published)

Country

**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](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN) (NIS Directive). 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.[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.