IGF 2020

Best Practice Forum Cybersecurity

CALL FOR CONTRIBUTIONS

Introduction

The IGF Best Practice Forum on Cybersecurity is a multistakeholder group focusing on identifying best practices in Cybersecurity.

Last year, the BPF published research 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, the Tech Accord, the Agreement on cooperation in ensuring the International Information Security between the Member States of the Shanghai Cooperation Organization and the 2015 UNGGE proposed norms. **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 . (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 (.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' (.pdf) published by the BPF's workstream 2.

CONTRIBUTION ASPI

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?

ASPI signed the Paris Call in 2018. As a think tank, we are studying national, regional and international cybersecurity with the intent of providing creative and innovative policy recommendations to remedy concerns and risks. A part of our work in cyber capacity building is to support greater socialisation and understanding of the cybersecurity norms and, in particular, the 2015 UNGGE norms in our region.

One area the BPF could additionally look at are ASEAN process, which include the ASEAN Ministerial Conference on Cybersecuirty (AMCC), the ASEAN Regional Forum (ARF) and its inter-sessional meeting on ICT secuirty, the ASEAN Defence Ministers Plus Expert Working Group on Cyber Security. The AMCC process is probably the most active after Singapore initiated this in 2018. Although the AMCC fundamentally builds on the UNGGE 2015 recommendations, it has set in motion a regional ASEAN-based approach to regional cybersecurity.

Another area BPF could look at is the South Pacific. The Pacific Islands Forum Boe Declaration in 2018 includes one line on regional cybersecurity. Activities on the ground amount to a broadening and deepening of this statement which implicitly reflect the portee of the some of the intergovernmental and indusrty norms. An example is the establishment of the PacSON network of incident responders/response team in the Pacific. Even in the absence of formal agreements, there are standing and developing practices that could be considered to constitute de facto norms-based arrangements.

2. What projects and programs have you implemented to support norms agreements your organization has agreed with?

ASPI is managing a cyber capacity building project that looks to support ASEAN governments with the implementation of the norms as recommended in the 2015 UNGGE report. The project includes training activities, awareness-raising materials and country-specific 'norms implementation reports'. Information is available at www.aspi.org.au/cybernorms

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: subsequent chairs' statements of the ASEAN Ministerial Conference on Cybersecurity
- Date of launch: from 2016
- Stakeholders party to the agreement: ministers responsible for cybersecurity from all member states of ASEAN
- Number or link to list of signatories: https://www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean
- Which organization maintains the agreement? If possible, provide contact information: Singapore Cybersecurity Agency
- Does the agreement include any of the following UN-GGE consensus norms? The AMCC participants have all subscribed in principle to the norms from the 2015 UNGGE report.

- Name of agreement: EAS leader's statement on deepening cooperation in the security of ICTs and of the digital economy
- Date of launch: November 2018
- Stakeholders party to the agreement: Member States of the Association of Southeast Asian Nations (ASEAN), Australia, the People's Republic of China, Republic of India, Japan, Republic of Korea, New Zealand, the Russian Federation and the United States of America.
- Number or link to list of signatories:
  - https://asean.org/storage/2018/11/EAS-Leaders%E2%80%99-Statement-on-Deepening-Cooperation-in-the-Security-of-ICT-a....pdf
- Which organization maintains the agreement? If possible, provide contact information: ASEAN
- Does the agreement include any of the following UN-GGE consensus norms? The statement refers to the 2015 UNGGE report.

Name of agreement: Boe Declaration on Regional Security, Pacific Islands Forum
- Date of launch: 2018
- Stakeholders party to the agreement: member states of the Pacific Islands Forum
- Number or link to list of signatories:
  - https://www.forumsec.org/2018/09/05/boe-declaration-on-regional-security/

- Which organization maintains the agreement? If possible, provide contact information: Forum Secretariat
- Does the agreement include any of the following UN-GGE consensus norms? The declaration lists cybersecurity as one area of emphasis, next to human security, environmental security and transnational crime, as part of an expanded concept of security which addresses the wide range of security issues in the region, both traditional and non-traditional. The Boe Declaration does not refer to the GGE norms but does imply similar elements like states and regional bodies being able to:
  - develop national security strategies; and strengthening national security capacity including through training.
  - identify and address emerging security challenges;
  - improve coordination among existing security mechanisms;
  - facilitate open dialogue and strengthened information sharing;
  - further develop early warning mechanisms;
  - support implementation;
  - promote regional security analysis, assessment and advice; and,
  - engage and cooperate, where appropriate, with international organisations,partners and other relevant stakeholders.

4. Are there cybersecurity issues you believe should be addressed by a cybersecurity agreement which are currently not?

   Cyber capacity building is emerging as a global priority in international cybersecurity, partly reflected by the latest draft OEWG report. But cyber capacity building efforts and investments in ICT infrastructure also become increasingly subject to competition over ideological influence, norms interpretation and other political and economic factors. Normative agreements on responsible and professional cyber capacity building design, programming and implementation may be needed. In that light, there should also be more attention to the impact of proposed cybersecurity measures, and their sustainability, in digitally developing economies and nations.

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', the BPF's draft research paper 'Exploring Best Practices in Relation to International Cybersecurity Agreements', or to suggest ways forward for the BPF in 2021.

The ‘what policymakers can learn’ paper is very well written and highly informative. I’d be interested to see how this document can be more widely shared and available. In addition, the document may benefit from more substantial recommendations: what is recommended to policymakers, what is recommended to industry etc.

At the following link (https://www.aspi.org.au/report/sydney-recommendations-practical-futures-cyber-confidence-building-asean-region) you find an ASPI publication on cyber confidence building measures that was published in 2018 which includes practical recommendations for each stakeholder group.

Furthermore, we'd be interested to explore how our work (see (2)) could complement this work of the BPF and vice versa.

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 Bart Hogeveen

Affiliation Australian Strategic Policy Institute, International Cyber Policy Centre

E-mail (for contact only/will not be published) barthogeveen@aspi.org.au

Country Australia

Annex A: List of agreements for consideration

- The G20, in their Antalya Summit Leaders' Communiqué, 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, 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 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 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 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 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 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 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, 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 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, 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 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). 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, 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.
- 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. 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), 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
- The Siemens Charter of Trust contains several product development norms, such as "user-centricity" and "security by default"
- GCSC Six Critical Norms - At the time of writing, the six critical norms are still in draft, and published for public input.