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 EastWest Institute

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)*

EastWest Institute is a signatory to the following agreements covered in Annex A:

- The Global Commission on the Stability of Cyberspace Final Report, *Advancing Cyberstability*. The final report includes eight proposed norms, along with principles and recommendations for cyberstability for both state and non-state actors (see suggested updates in Question 3).
- Paris Call for Trust and Security in Cyberspace
    - To note, the Paris Call is covered in the Exploring Best Practices in Relation to International Cybersecurity Agreements background paper, but is not included in Annex A.

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

There are two main project areas where EWI is working to support the implementation of norms agreements:

Global Cyber Policy Dialogues: Launched in 2020, this project seeks to convene multistakeholder dialogues on a regional basis to build cyber networks, facilitate information exchange on addressing cyber challenges, and support capacity building with a view to specifically complement the implementation of cyber norms and ongoing UN OEWG and GGE processes. The regional dialogues are intended to engage thought leaders and policy makers in developing countries to generate practical policy approaches to address cyber challenges. In support of the operationalization and implementation of cyber norms, the project seeks to broaden the international conversations around cyber norms to better incorporate the priorities, concerns and approaches of developing countries. A related goal is to support cyber capacity building by facilitating cross-sectoral networks, developing regional capacity building agendas, and identifying where current norms and international agreements can be integrated into national and regional level efforts to address cyber challenges.

Work to curb "technology nationalism" and improve trust and security in ICT supply chains: Ensuring security in global ICT supply chains is essential for trust in the Internet and society's widespread use of ICT. The 2015 GGE norm to "ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products" underscores this point. In early 2020, EWI published a report, *Weathering TechNationalism: A Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk*. This report offers an assurance, trust and accountability framework for addressing ICT supply chain security in a holistic way. It includes suggested measures at the organizational, industry and ecosystem levels, including security baseline requirements and best practices, the development of international standards and norms, coordinated vulnerability disclosure, establishments of transparency centers, and global conformance programs. Following the launch of the report, EWI has been engaging stakeholders to promote technical and operational measures to increase trust in global ICT supply chains, and where these methods are insufficient, examining what confidence-building measures and norms could help fill the "trust gap." This work supports the implementation of the GCSC norms to avoid tampering and prevent and mitigate significant vulnerabilities, as well as the Siemens Charter of Trust, Cybersecurity Tech Accord, and other private sector transparency initiatives. In addition to norms and confidence-building, this work also includes a capacity building element, as there are different levels of preparedness across stakeholder groups—such as small and medium-sized enterprises that are part of the global supply chain—and developing countries, that may not have the same level of resources to assess and address supply chain risks.

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

We would suggest updating the Global Commission on the Stability of Cyberspace contribution to include the Commission's final report, *Advancing Cyberstability*. Below are suggested updates based on what is currently listed in the draft research paper, "Exploring Best Practices in Relation to International Cybersecurity Agreements."

- Name: Global Commission on the Stability of Cyberspace Cyberstability Framework
  This suggested edit updates the current reference from the Six Critical Norms originally released in 2017, to include all eight norms elaborated in the Commission's final report from November 2019, as well as the overall Cyberstability Framework, which includes several underlying principles (human rights, requirement to act, restraint and responsibility).
- Updates to UN GGE norms that are covered in this agreement:
    - States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack
      Not listed in the eight norms, but included in the principle of Requirement to Act, which is a "general requirement to take affirmative action to preserve the stability of cyberspace." It also includes a provision for non-state actors (companies, individuals) to take cooperative action to preserve the stability of cyberspace, including working together to mitigate cyber threats.

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', 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 "Exploring Best Practices" paper is a great initiative and useful resource to see how the 2015 UN GGE norms reflect an emerging consensus through other international and regional agreements!

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 Abagail Lawson

Affiliation EastWest Institute

E-mail (for contact only/will not be published) alawson@eastwest.ngo

Country USA

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.